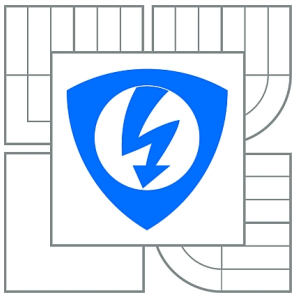
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

SYSTÉM PRO MĚŘENÍ KVALITY ELEKTRICKÉ ENERGIE

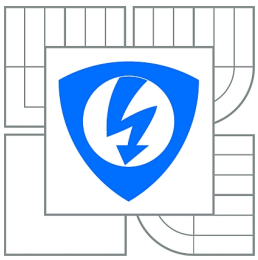
POWER QUALITY MEASURING SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. JAROSLAV VALENTA
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR MLÝNEK
SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Jaroslav Valenta	***ID:***	98677
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Systém pro měření kvality elektrické energie

POKYNY PRO VYPRACOVÁNÍ:

V rámci diplomové práce navrhněte a realizujte simulační model sběrné sítě dálkového měření kvality elektrické energie. Dále pak vytvořte knihovny, pomocí kterých bude možné zabezpečit datovou komunikace ze sběrných míst dálkového měření.

DOPORUČENÁ LITERATURA:

[1] Blažek, V., Skala, P.: Distribuce elektrické energie. Skriptum VUT v Brně, FEKT.
[2] ČSN EN 50160: Charakteristiky napětí elektrické energie dodávané z veřejné distribuční sítě, červen 2000.
[3] Burda.K.: Bezpečnost informačních systémů. Skripta FEKT VUT v Brně, 2005.

Termín zadání:	7.2.2011	***Termín odevzdání:***	26.5.2011

Vedoucí práce: Ing. Petr Mlýnek

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

ANOTACE

Tato práce se zabývá problematikou měření kvality elektrické energie. Budou rozebrány parametry, dle kterých se kvalita hodnotí, dále budou popsány systémy dálkového sběru dat a s nimi spojené technologie přenosu. V dnešní době by se také nemělo zapomínat na zabezpečení přenášených dat. Z tohoto důvodu budou také popsány a testovány nejrůznější druhy kryptografických algoritmů. Budou realizovány kryptografické algoritmy, pomocí kterých je možné zabezpečit datovou komunikaci ze sběrných míst dálkového měření. Kryptografické algoritmy budou realizovány nejprve v simulačním prostředí MATLAB a následně v jazyce C/C++. V poslední části práce je navržen a realizován simulační model sběrné sítě dálkového měření kvality elektrické energie.

Klíčová slova:

PLC, RSA, Diffie-Hellman, kvalita elektrické energie, simulační model

ABSTRACT

This thesis deals with the measurement of power quality. The evaluating quality parameters, data collection systems and transfer technologies will be discussed. The various type of cryptographic algorithms are also described. Cryptographic algorithms, which ensure to secure data communications from remote collection points of measurement, will be realized. These cryptographic algorithms will be realized in MATLAB and C/C++. The last part is focus on designed and implemented a simulation model to telemetry the power quality.

Keywords:

PLC, RSA, Diffie-Hellman, power quality, simulation model

VALENTA, J. *Systém pro měření kvality elektrické energie.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 55 s. Vedoucí diplomové práce Ing. Petr Mlýnek.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma "Systém pro měření kvality elektrické energie" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce Ing. Petru Mlýnkovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování práce.

V Brně dne .....……. .....
podpis autora

OBSAH

ÚVOD

V dnešní době se stále větší důraz klade na kvalitu elektrické energie, a proto je velmi důležité mít k dispozici kvalitní prostředky, kterými je možno tuto kvalitu hodnotit. Právě těmito problémy se zabývá tato diplomová práce. Aby bylo možno objektivně hodnotit kvalitu elektrické energie, je potřeba mít k dispozici nějaké parametry, podle kterých by se kvalita hodnotila. Právě tyto parametry jsou popsány v úvodní části práce. Dále je potřebné naměřená data nějakým způsobem přenášet od koncových zařízení někam do sběrné centrály. Tímto problémem se zabývá další část práce, kde jsou popsány současné typy přenosových technologií. Samozřejmě by se neměla opomíjet ani bezpečnost přenášených dat. Z tohoto důvodu se bude další část práce věnovat zabezpečení dat. Budou popsány a testovány nejrůznější druhy kryptografických algoritmů.

Praktická část této práce je zaměřena převážně na bezpečnost přenášených dat. Pozornost bude zaměřena zejména na kryptografické algoritmy, pomocí kterých je možné zabezpečit datovou komunikaci ze sběrných míst dálkového měření. Budou testovány různé typy symetrických kryptografických algoritmů z hlediska časové náročnosti. Dále budou prakticky realizovány asymetrické kryptografické algoritmy. Tyto algoritmy budou realizovány nejprve v simulačním prostředí MATLAB a následně v jazyce C/C++. Díky realizaci v jazyce C/C++ je umožněna případná implementace do reálných zařízení.

Pro lepší přehlednost a ověření funkčnosti budou také vytvořeny uživatelské aplikace, pomocí kterých lze jednoduše odzkoušet funkčnost vytvořených algoritmů. V poslední části práce bude realizován simulační model sběrné sítě dálkového měření kvality elektrické energie. V rámci modelu bude řešen především problém, jakým způsobem zabezpečit autentičnost dat. Jinými slovy jak zabezpečit to, že data, která přišla z koncového zařízení do sběrného zařízení, opravdu pochází z příslušného koncového zařízení a nebyla při vlastním přenosu nějakým způsobem pozměněna. Pro stanovení klíčů je využit Diffie-Hellmanův kryptografický protokol.

1 PROBLEMATIKA MĚŘENÍ KVALITY ELEKTRICKÉ ENERGIE

Kvalita je charakteristika elektrické energie v daném bodě elektrické sítě vyhodnocená vzhledem k souboru referenčních technických parametrů. Všechny tyto parametry jsou definovány v normě ČSN EN 50160 „Charakteristiky napětí elektrické energie dodávané z veřejné distribuční sítě“ [4]. Na kvalitu elektrické energie mají vliv např. přenosové vlastnosti distribučních sítí, meteorologické jevy nebo spotřebiče připojené k elektrické síti. Špatná kvalita elektrické energie může způsobit ztráty ve výrobních procesech. Velikost ztrát je závislá na charakteru výroby. Jiný dopad bude mít krátkodobý pokles napětí u žhavící pece a jiný u citlivého přístroje v závodech přesné výroby.

1.1 Vybrané parametry kvality napětí podle ČSN EN 50 160

Kmitočet sítě pro sítě synchronně pracující s propojenou soustavou

Kmitočet síťového napětí se měří po dobu 10 s s rozlišením lepším než 10 MHz. Předepsaná doba měření je 1 týden, v jehož průběhu musí naměřené hodnoty splňovat následující tolerance:

50 Hz ± 1 % (tj. 49,5 ... 50,5 Hz) pro 99,5% naměřených 10 s hodnot

50 Hz + 6 % - 4 %(tj. 47 ... 52 Hz) pro 100% naměřených 10 s hodnot

Velikost napájecího napětí

Normalizované jmenovité napětí pro veřejnou síť nízkého napětí má efektivní hodnotu 230 V. Je to napětí fázové mezi fázovými vodiči a vodičem středním. Normalizovaná hodnota napětí sdruženého má efektivní hodnotu 400V. Pro síť s kmitočtem 50 Hz se hodnota napětí měří v časovém intervalu 10 cyklů. Měří se pravá efektivní hodnota (TRMS). Na hladině VN se hodnotí napětí sdružená a na hladině VVN napětí sdružená i fázová [1].

Odchylky napájecího napětí

Za normálních provozních podmínek musí být více než 95 % průměrných efektivních hodnot napětí, změřených v intervalech 10 min jednoho týdne, v rozsahu U_{jm} +6 % -10 % (tj. 207,0 V až 243,8 V) pro napětí fázové a (360 V až 424 V) pro napětí sdružené. Desetiminutová průměrná hodnota se vypočte ze 3000 hodnot napětí změřených za 10 period (0,2 s). Žádná 10 minutová hodnota napětí nesmí na NN vedeních normální délky překročit toleranci 230 V + 10 % -15 % (tj. 195,5 V až 253 V) [1].

Rychlé změny napětí

Rychlá změna napětí je rychlý přechod efektivní hodnoty mezi dvěma ustálenými stavy. Rychlé změny napětí jsou způsobovány zejména změnami zatížení u odběratelů nebo spínáním v síti, kdy se napětí pohybuje v dovolených tolerancích, avšak jeho změny vyvolávají nepříznivé účinky u spotřebičů. Pro měření rychlých změn napětí se musí definovat minimální rychlost změny, minimální doba ustáleného stavu a minimální rozdíl mezi dvěma ustálenými stavy [1].

Flikr

Periodické změny efektivní hodnoty napětí, i když se napětí nalézá v dovolených tolerancích, se mohou projevit jako blikání světelných zdrojů, tzv. flikr. Flikr je charakterizován dvěma parametry a to P_{st} (krátkodobý flikr – 10 min) a P_{lt} (dlouhodobý flikr – 2 hod). V normě ČSN EN 50160 je předepsáno, že dlouhodobá míra vjemu flikru P_{lt} musí být po 95% času týdenního měření menší než 1,0. Koeficienty P_{st} (short time) i P_{lt} (long time) jsou bezrozměrné [1].

Krátkodobé poklesy napětí (doba trvání do 1 s a do 60 % Un)

Krátkodobé poklesy napájecího napětí jsou obecně způsobeny zkraty. U odběratelů vzniká cca 60 % zkratů a zbytek má původ v distribučních sítích. Jejich četnost se v průběhu roku může značně měnit a závisí na typu distribuční sítě a charakteru připojených spotřebičů. Většina poklesů trvá dobu kratší než 1 s (vypnutí zkratu vláknovou pojistkou nastává za cca 10 ms, jističem cca 100 ms, VN ochranou od 0,2 s do 1,0 s podle napěťové hladiny). Krátkodobý pokles je charakterizován svou hloubkou a dobou trvání. Normou doporučená doba měření událostí je 1 rok, a proto je vhodné u všech událostí registrovat čas vzniku události [1].

Krátkodobá a dlouhodobá přerušení napájecího napětí

Přerušení napájecího napětí je definováno jako stav, kdy napětí klesne pod prahovou hodnotu. V normě ČSN EN 50160 se uvádí hodnota 1 % U_{jm}, v aktualizovaných provozních předpisech se přechází na 5 % U_{jm}. U trojfázového vývodu nastává přerušení až tehdy, když všechna tři napětí klesnou pod prahovou hodnotu a přerušení končí, jakmile alespoň jedno napětí vzroste nad prahovou hodnotu. Hranice mezi krátkodobými

a dlouhodobými přerušeními není také jednotná. Některé dokumenty uvádějí dobu 1 min, jiné 3 min. Celosvětově se odhaduje, že poklesy, dočasná přepětí a přerušení napětí způsobují cca 80 % ekonomických ztrát způsobených nekvalitním napětím. Bohužel opatření na snížení počtu a dob trvání těchto událostí jsou nejnákladnější a nejhůře realizovatelná, a proto je nezbytně nutné věnovat tomuto parametru pozornost již v době projektování [1].

Dočasná přepětí o síťovém kmitočtu mezi živými vodiči a zemí

Dočasná přepětí o síťovém kmitočtu mezi živými vodiči a zemí vznikají při zemních poruchách. V uzemněných soustavách se napětí nezvýší nad 1,71 U_{jm}. V izolovaných soustavách nebo při rezonancích může vzniknout dočasné přepětí i vyšší než 2 U_{jm}. Nejčastěji vznikají dočasná přepětí při regulacích napětí v odtíženém stavu [1].

Přechodná přepětí mezi živými vodiči a zemí

Jedná se o transientní přepětí způsobená spínacími pochody nebo atmosférickými vlivy. Spínací přepětí nejsou obvykle tak strmá jako přepětí atmosférická. Mají vesměs také delší dobu trvání. Pro měření přechodných přepětí se používají samostatné speciální vf měřicí přístroje. V normě ČSN EN 50160 se neuvádí limitní hodnoty ani počty těchto přepětí [1].

Nesymetrie napájecího napětí

Napěťová nesymetrie má vliv na snížení výkonů motorů. V normálních provozních podmínkách sítě NN musí být v libovolném týdenním období 95 % desetiminutových středních efektivních hodnot zpětné složky napájecího napětí v rozsahu do 2 % složky sousledné. Pro trojfázové systémy se v normě ČSN EN 61000-4-30 používá k výpočtu nesymetrie vztahů :

$$Uz = \sqrt{\frac{1-\sqrt{3-6\beta}}{1+\sqrt{3-6\beta}}}, \tag{1.1}$$

$$kde\ \ \beta = \frac{U_{12}^4 + U_{23}^4 + U_{31}^4}{\left(U_{12}^2 + U_{23}^2 + U_{31}^2\right)^2}. \tag{1.2}$$

Harmonická napětí

Podstatou vzniku harmonických je odběr neharmonického (tedy impulzního nebo nesinusového) proudu tzv. nelineárními zátěžemi. Příkladem těchto zátěží mohou být pohony s variabilní rychlostí používající napěťový střídač, dále pak tavicí pece v metalurgii, elektronické předřadníky svítidel apod. [5]. Pro výpočet harmonických napětí se používají algoritmy FFT. Za normálních provozních podmínek musí být 95 % desetiminutových středních efektivních hodnot napětí každého harmonického napětí menší nebo rovno hodnotě uvedené v tabulce 1.1. Činitel tvarového zkreslení THD (Total Harmonic Distortion) harmonických složek do řádu 40 včetně musí být v NN síti menší nebo roven 8,0 % U_{jm}. Celkové harmonické zkreslení THD se v normě ČSN EN 50160 počítá dle vztahu

$$THD = \sqrt{\sum_{n=2}^{40} \left(\frac{Un}{U1} \right)^2} , \tag{1.3}$$

kde $U1$ je velikost napětí první (základní) harmonické složky napětí,

Un je velikost napětí n-té harmonické složky napětí.

Tabulka 1.1 Hodnoty jednotlivých harmonických napětí v procentech U_{jm} pro řády harmonických až do 25.

Liché harmonické ne násobky 3		**Liché harmonické násobky 3**		**Sudé harmonické**	
Řád harmonické n	Harmonické napětí %	Řád harmonické n	Harmonické napětí %	Řad harmonické n	Harmonické napětí %
5	6,0	3	5,0	2	2,0
7	5,0	9	1,5	4	1,0
11	3,5	15	0,5	6…24	0,5
13	3,0	21	0,5		
17	2,0				
19	1,5				
23	1,5				
25	1,5				

Meziharmonická napětí

Ve frekvenčních pásmech mezi harmonickými složkami se vyskytují meziharmonická napětí, která nejsou zanedbatelná zvláště v provozech s frekvenčními měniči. V normě ČSN EN 61000-4-7 je uveden kmitočtový interval mezi dvěma po sobě jdoucími meziharmonickými spektrálními čarami o velikosti 5 Hz. V normě jsou také definovány metody seskupování meziharmonických napětí do skupin. Rozlišuje se zde skupina harmonických, skupina meziharmonických a vycentrovaná skupina meziharmonických. Pro hodnoty meziharmonických nejsou zatím definovány směrné hodnoty [1].

Napětí signálů v napájecím napětí

Distribuční síť je využívána k přenosu informací. V rámci normy ČSN EN 50160 se jedná o systémy pracující v pásmu kmitočtů do 2 kHz. I když v poslední době jsme svědky diskusí a ověřování systémů, u nás se běžně používá tzv. systém hromadného dálkového ovládání HDO, který nejčastěji pracuje s kmitočtem 216 Hz. Pro hodnocení vlivu signálu HDO na kvalitu napětí se používají meziharmonické složky 210 Hz, 215 Hz, 220 Hz a 225 Hz, z nichž se používají průměrné hodnoty za dobu 3 s. Norma předepisuje, že 99 % těchto 3 s hodnot musí být při kmitočtu 216 Hz menší než 9 % U_{jm} [1].

2 DÁLKOVÉ MĚŘENÍ KVALITY ELEKTRICKÉ ENERGIE

V dnešní době se stále více využívá možností dálkového sledování kvality elektrické energie u odběratele, dálkových odečtů měřicích přístrojů, využívá se možností dohledových center pro provoz sítí, rozšiřují se bezobsluhové rozvodny. Pro dálkové odečty z měřicích přístrojů jsou v současné době využívány různé možnosti. Nejčastěji používané jsou především vlastní komunikační okruhy, které mohou být realizovány například pomocí technologií PLC, GSM, INTERNET apod. Musí být ovšem kladen důraz především na spolehlivost komunikace a ochranu před neoprávněným přístupem k datům a ovládacím prvkům.

2.1 Systémy AMR, AMM, AMI

V posledních letech v souvislosti s rozvojem technologie inteligentního měření vzniklo několik nových pojmů, ale přesná definice pojmu inteligentní měření není zcela jasná. Mnoho dodavatelů technologií inteligentního měření používá svůj vlastní výklad. V dnešní době průmysl v podstatě rozlišuje tři následující pojmy (AMR, AMM, AMI) [6].

AMR (Automated Meter Reading)

Je to systém jednosměrné komunikace mezi centrálním systémem a jednotlivými měřicími místy. Umožňuje provádět dálkové odečty hodnot, které jsou založeny na pokročilé technologii, která umožňuje odečítat naměřené hodnoty na dlouhé vzdálenosti. Díky AMR lze odečítat roční, měsíční, týdenní, denní nebo hodinovou hodnotu měřeného parametru. Naměřené hodnoty a údaje o stavu, jako jsou například časová razítka, jsou přenášeny pomocí různých přenosových technologií do centrálního systému, kde je provedena analýza [6].

AMM (Automated Meter Management)

Je to systém komunikace mezi centrálním systémem a jednotlivými měřicími místy. Komunikace je oproti AMR obousměrná a zpravidla ji řídí centrální systém. Pomocí AMM se mohou monitorovat nejrůznější měřené parametry v každém měřicím místě. Zajišťuje i to, že v případě neoprávněného zásahu do měřicího přístroje nebo komunikačního vedení je místo snadno odhaleno. Základem systému AMM je Smart Meter, který měří nejrůznější parametry sítě. Jeho součástí je i zabezpečení, zda naměřená data jsou kompletní a také ochrana před neoprávněnými zásahy. To bývá realizováno různými kontrolními výpočty a snímači, které dokáží signalizovat otevření

krytu svorkovnice, nebo měřicího přístroje. Základní systém AMM umožňuje měření, monitorování a řízení všech měřicích míst. Důraz je kladen zejména na jednoduchost systému sběru dat a na dostupnost informací. Většina akcí se také obejde bez nutnosti návštěvy provozních techniků na měřicím místě [7].

AMI (Advanced Metering Infrastructure)

Infrastruktura prostředků pro podporu AMR a AMM, tj. podpora vývoje v oblasti elektroměrů, komunikací a systémů s důrazem na otevřenost a užití mezinárodních standardů, včetně managementu nasazování řešení.

2.2 Koncept dálkového měření

Dálkovým měřením a odečty se v dnešní době zabývá mnoho firem. Na našem trhu například *Landis+Gyr* [16], *Actaris* [17], *ModemTec* [11] a jiné. Proto se také nabízí mnoho způsobů pro realizaci systému dálkového sběru dat. Při realizaci konceptu systému dálkového měření kvality elektrické energie bylo vycházeno ze stávajícího systému ISAR od firmy *ModemTec.* Byl vytvořen koncept systému, který využívá prvky systému ISAR v kombinaci s měřiči kvality elektrické energie PQmetr od firmy *MEgA*. Systém ISAR je automatizovaný systém dálkového sběru dat. Může být použit pro dálkové odečty spotřeby plynu, vody, elektřiny, detekci neoprávněných odběrů, či odpojení nebo připojení spotřebitele. Koncová zařízení PQ monitory jsou měřicí přístroje pro měření parametrů kvality napětí dle ČSN EN 50160. Navržený koncept systému využívá přenosové technologie PLC a GPRS, které budou popsány v kapitole 3.

2.2.1 Komponenty systému

Navržený systém pro měření kvality elektrické energie se skládá z následujících komponentů:

- Měřiče kvality elektrické energie PQ monitor
- Externí komunikační jednotky MT-29N
- Koncentrátory DK - MT100
- Agregační počítačový server s centrálním systémem

Měřič kvality elektrické energie PQ monitor

PQ monitor je měřicí přístroj pro měření parametrů kvality napětí dle ČSN EN 50160. Je schopen měřit až 4 napětí a 4 proudy nebo i jiné veličiny. Zaznamenává nejen normou definované charakteristiky událostí na napětích, ale i průběhy všech čtyř napětí i proudů

na počátku a na konci každé události, tzv. počáteční a koncový detail. PQ monitor umožňuje na základě změřených průběhů proudů určit směr vzniku události i flikru. Dále umožňuje také monitorovat napětí mezi středním vodičem a harmonickou analýzu proudu středního vodiče. PQ monitor má na výstupu přepínací kontakt polarizovaného relé s možností naprogramovat význam signalizace [12].

PQ monitor je navržen v těchto konstrukčních provedeních:

MEg 30 - PQ monitor v přenosném provedení pro sítě NN,
MEg 31 - PQ monitor v přenosném provedení pro sítě VN,
MEg 32 - PQ monitor v provedení pro pevnou montáž v sítích NN,
MEg 33 - PQ monitor v provedení pro pevnou montáž v sítích VN.

Externí komunikační jednotka MT29-N

Externí komunikační jednotka MT29-N slouží k obsluze měřiče kvality elektrické energie PQ monitoru. Jednotka má k dispozici 6 vstupů pro připojení mechanických bezpotenciálových spínačů, jazýčkových, nebo jiných relé, nebo tranzistorů s otevřeným kolektorem i emitorem. Je také vybavena čtyřmi bezpotenciálovými výstupy, které tvoří spínací kontakty relé. Pro komunikaci s prostředím lze využít dvě sériové linky RS232, které nejsou galvanicky odděleny od systému, ale jsou galvanicky odděleny od síťového napětí 230 V. Jednu linku je možno využít pro komunikaci se zařízeními, která předávají data ke zpracování. Druhá linka slouží k připojení PC, komunikační jednotky, nebo k propojení na jiný komunikační uzel [11].

Koncentrátor DK - MT100

Koncentrátor tvoří mezistupeň komunikace mezi centrálním systémem a jednotlivými odběrnými místy. Ukládají se zde dočasně data z měřicích zařízení, v našem případě PQ monitorů, v okruhu jednoho distribučního transformátoru. Zařízení se umísťuje do plechové skříně s krytím IP65, v přímé blízkosti distribučního transformátoru na straně NN [11].

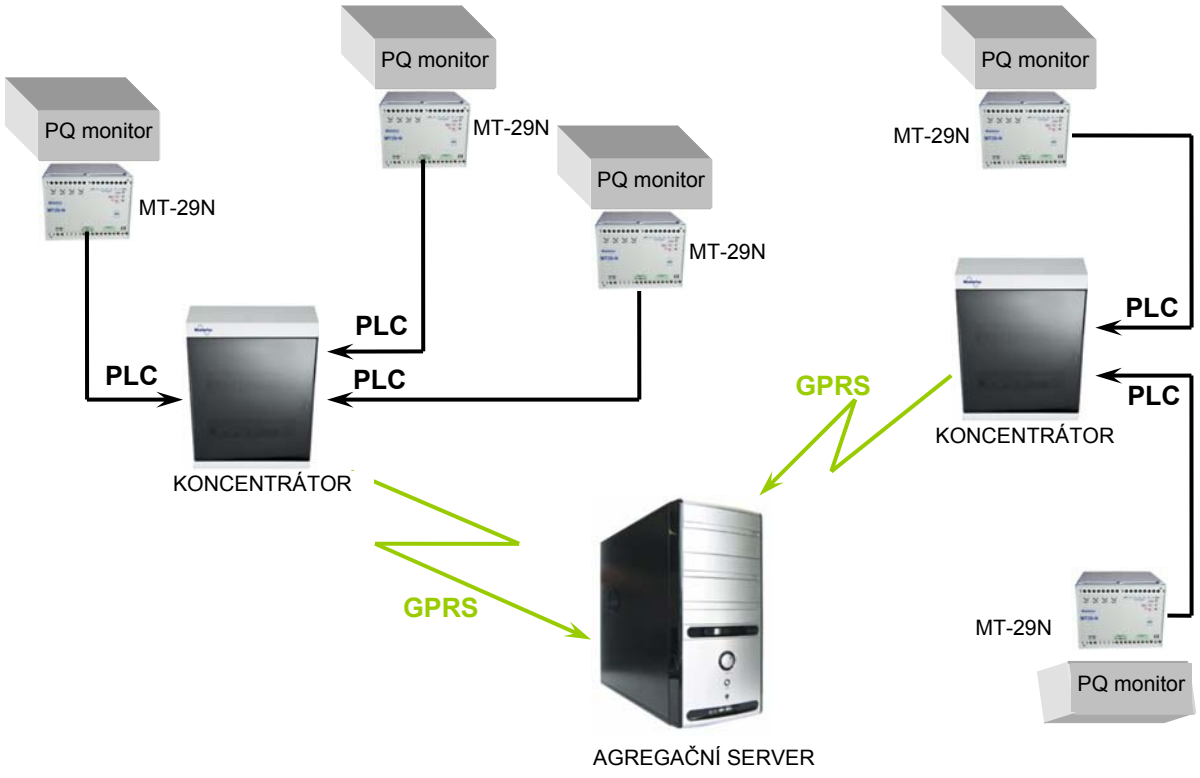
Agregační server

Agregační server je centrem systému. Jedná se o počítačový server s programovým vybavením a komunikačním rozhraním pro spojení s koncentrátory. Automaticky sbírá a ukládá data z jednotlivých odběrných míst měřené sítě.

Základní vlastnosti

- Optimalizovaný úsporný TCP protokol pro komunikaci s koncentrátorem (vhodný i pro GSM přenos)
- Vzdálená konfigurace koncentrátorů, aktualizace softwaru koncentrátoru
- Šifrovací VPN server pro zajištění zabezpečení a komprimace komunikace mezi koncentrátorem a agregačním serverem
- Programování automatizovaných činností měřiče (nastavování kalendáře, plánování odečtových záznamů)
- Vyhodnocování výsledků měřených dat a generování událostí (např. ztráta komunikace, …)
- Upozorňování na události (odesláním emailu, prozvoněním telefonu)
- Řízení sběru dat z více koncentrátorů v případě mřížových sítí
- XML rozhraní pro poskytování služeb a dat v agregačním serveru jiným systémům
- Zálohování systému bez přerušení ostatní činnosti
- Součástí agregačního serveru může být také integrovaný koncentrátor (např. v případě malé lokality) [11].

2.2.2 Princip systému



Obrázek 2.1 Systém pro dálkové měření kvality elektrické energie.

Každý měřicí přístroj je připojen ke komunikační jednotce. Tato jednotka dále data přenáší pomocí technologie PLC do koncentrátoru. Princip technologie PLC bude popsán v kapitole 3.1. Systém může pomocí technologie PLC vysílat v kmitočtovém pásmu 70 kHz až 148,5 kHz, s výjimkou pásma C. Jedná se o úzkopásmový, fázově modulovaný přenos se šířkou pásma 10 kHz. PLC technologie umožňuje přenos dat z celé oblasti pokryté distribuční trafostanicí a to i v silně zarušeném prostředí. To je dáno tím, že maximální délka NN vedení z transformátoru, po kterém jsou přenášeny data, zpravidla nepřesahuje 2–3 km, což je vzdálenost na kterou PLC komunikační jednotky spolehlivě komunikují. Tím pádem odpadá nutnost nákladné pokládky kabeláže. Po přenosu údajů do koncentrátoru následuje jejich přenos do agregačního serveru. Toto může probíhat např. pomocí technologie GPRS, jejíž princip je popsán v kapitole 3.2. Agregační počítačový server automaticky sbírá, ukládá a analyzuje data z jednotlivých odběrných míst měřené sítě [11].

3 PŘENOSOVÉ TECHNOLOGIE

V rámci této kapitoly budou popsány přenosové technologie PLC a GPRS, které se používají k přenosu naměřených dat z koncových zařízení do sběrných zařízení.

3.1 Technologie PLC

Komunikace po silových vedeních PLC využívá pro přenos dat stávající elektrickou síť. To je značně výhodné zejména z hlediska dostupnosti. Princip přenosu dat po silových vedeních spočívá v tom, že galvanickým oddělením a odfiltrováním například (230 V, 50 Hz), můžeme po silovém vedení přenášet signály vyšších frekvencí, které mohou díky vhodné modulaci přenášet data. Mezi výhody přenosu dat po PLC paří to, že se nemusí budovat žádná přenosová trasa a přenos informací není nijak zpoplatněn. Jako nevýhodu lze uvést, že silové vedení má jako komunikační kanál značně proměnné parametry, které mohou způsobit velké problémy při přenosu, případně znemožnit přenos úplně. V energetických sítích může být realizován jak úzkopásmový, tak i širokopásmový přenos dat. Pro potřebu přenosu telemetrických údajů se využívá přenos úzkopásmový [8].

3.1.1 Úzkopásmový přenos dat pomocí PLC

Úzkopásmový přenos dat po silových vedeních může být využit nejen pro dálková měření, ale také pro dálkové ovládání například domovního topení, klimatizace nebo některých domácích spotřebičů. Data jsou pomocí úzkopásmového přenosu přenášena malými rychlostmi, řádově několik stovek kbps. Tyto rychlosti jsou však pro přenos telemetrických údajů dostačující [8].

3.1.2 Normalizace úzkopásmových služeb

V České republice se úzkopásmový přenos dat po energetických sítích řídí normou CENELEC EN 50065. Rozdělení kmitočtů pak ukazuje následující tabulka [8].

Tabulka 3.1 Rozdělení kmitočtů.

Pásmo	Kmitočtový rozsah	Poznámka
	3 až 95 kHz	jen pro dodavatele el. energie
A	9 až 95 kHz	Pro dodavatele el. energie a po jejich souhlasu i pro odběratele
B	95 až 125 kHz	Jen pro odběratele
C	125 až 140 kHz	Jen pro odběratele – vyžadován protokol o přistoupení k dohodě
D	140 až 148,5 kHz	

3.1.3 Princip úzkopásmového přenosu po PLC

Pro přenos naměřených údajů po silových vedeních jsou potřeba 2 základní prvky. **Modem**, který data z měřicího zařízení odesílá a **koncentrátor**, který odeslané data přijímá a následně ukládá. Koncentrátor dále může odesílat data k vyhodnocení někam do řídicího systému. Do koncentrátoru se ukládají data v rámci okruhu jednoho transformátoru, protože transformátor je pro data přenášená pomocí PLC nepřekonatelnou překážkou. Koncentrátory se umisťují v blízkosti trafostanice na stranu nižšího napětí. PLC modem by se kvůli svému dosahu neměl nacházet ve vzdálenosti větší, než 3 km od koncentrátoru, aby nedošlo ke ztrátě přenášených dat [8].

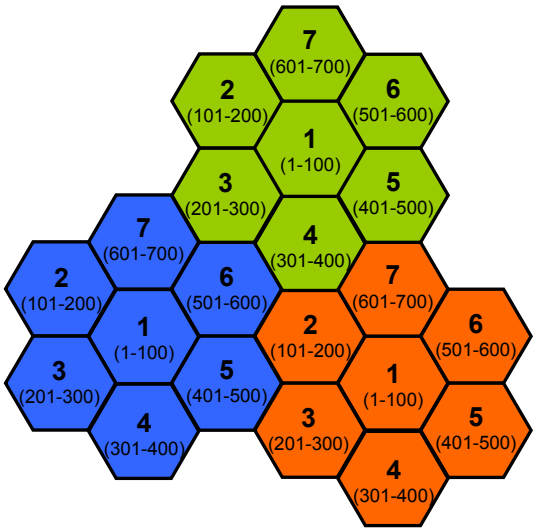
3.2 Technologie GSM

Technologie GSM je velmi rozšířený standard využívaný převážně pro mobilní komunikaci. Jedná se tedy o technologii bezdrátovou, která je velmi rozšířená. V České republice tato technologie pokrývá 98 % území. Technologie GSM umožňuje jak hlasové, tak datové přenosy. Pro naši potřebu dálkového sběru dat však bude v této práci pozornost věnována pouze datovým službám. Systém GSM umožňuje i přenos paketových dat, což umožnila implementace technologie GPRS. Vyšších přenosových rychlostí bylo dosaženo pomocí technologií EDGE a UMTS. V případě technologie UMTS se už jedná o třetí generaci systému mobilních telefonů.

3.2.1 Základní princip systému GSM

Mobilní sítě využívají ke své činnosti rádiové vlny. Ovšem frekvence, které jsou pro ně dostupné, jsou omezeny a každý mobilní operátor jich získává jen omezený počet. Rozsahy frekvencí přidělené mobilním operátorům nikdy nemohou postačovat na to, aby operátor mohl přidělit každému datovému přenosu samostatný komunikační kanál (rozsah frekvencí). Každý kanál je dále rozdělen na 8 timeslotů. Řešením takového nedostatku frekvencí je vícenásobné použití stejných frekvencí, tzn. aby různé datové přenosy používaly stejné frekvence, ale zároveň se vzájemně neovlivňovaly. K tomu se využívá tzv. buňkový (celulární) systém. Podstata tohoto systému je rozdělení území, na kterém operátor poskytuje své služby, na části (buňky), které jsou uspořádány tak, že rozsah frekvencí (kanály) využívané v jedné buňce nejsou využívány v žádné ze sousedních buněk (viz obrázek 3.1). Takovýmto způsobem lze s omezeným počtem frekvencí pokrýt libovolně velké území. Eventuelní potřeba zvýšení počtu datových přenosů je nutná řešit hustější sítí buněk. V každé buňce je umístěna základnová stanice

BTS, jejímž úkolem je komunikovat s koncovými zařízeními, které se nachází uvnitř příslušné buňky [9], [10].



Obrázek 3.1 Vícenásobné využití přidělených kmitočtů.

3.2.2 Přenos datových signálů v systému GSM

Systém GSM umožňuje ve své základní variantě přenos datových signálů s přenosovou rychlostí až 9,6 kbps. Díky flexibilitě systému GSM a implementaci nových standardů GPRS, HSCSD a EDGE, je však možné systémem GSM přenášet datové signály přenosovými rychlostmi v řádu desítek až stovek kbps [10].

Klasický přenos dat v systému GSM

Způsob kódování dat v systému GSM je poměrně složitý. Data musí být důkladně zabezpečena, neboť chyba v přenosu jediného bitu (např. desetinné čárky) se může projevit jako zcela chybný údaj. Pro přenos datových signálů existuje pět různých datových kanálů s označením TCH/F9.6, TCH/F4.8, TCH/F2.4, TCH/H4.8, a TCH/H2.4, které používají odlišné způsoby kanálového kódování i prokládání. Písmena TCH (Traffic Channel) označují provozní kanál, písmeno za lomítkem F (Full-Rate) resp. H (Half-Rate) značí přenos s plnou nebo poloviční rychlostí a desetinné číslo udává přenosovou rychlost signálu v kbps [10].

Tabulka 3.2 Přenosové rychlosti pro různé datové kanály.

označení kanálu	přenosová rychlost před kanálovým kódováním [kbps]	přenosová rychlost po kanálovém kódování [kbps]
TCH/F	13,0	22,8
TCH/F9.6	12,0	22,8
TCH/F4.8	6,0	22,8
TCH/F2.4	3,6	22,8
TCH/H4.8	6,0	11,4
TCH/H2.4	3,6	11,4

GPRS (General Packet Radio Service)

Pomocí systému GPRS lze stávající systém GSM rozšířit a umožnit tak přenos datových paketů přes rádiové rozhraní s teoretickou přenosovou rychlostí až 171,2 kbps. Aplikace technologie GPRS, založené na paketovém přenosu dat pomocí protokolu IP, umožňuje mobilní přístup do sítě internet. Protože stávající systém GSM neumožňuje paketový přenos dat, je nutné doplnění mobilní stanice i dalších částí systému GSM o nové bloky. Technologie GPRS je kompatibilní se současnými datovými sítěmi. Sítě s technologií GPRS se vzdálily původním sítím GSM, neboť využívají především jejich rádiovou část a přibližují se více datovým sítím a oblasti informačních technologií.

HSCSD (High Speed Circuit Switched Data)

Standard HSCSD specifikovaný ETSI umožňuje přenos dat v síti GSM vyšší rychlostí bez hardwarového zásahu do její struktury. Nejedná se tedy o paketový přenos dat. Úpravy sítě jsou pouze softwarovou záležitostí, což umožňuje velice rychlou implementaci HSCSD do stávajících sítí. Vyšší přenosové rychlosti je dosaženo novým způsobem kódování, který umožní zvýšit přenosovou rychlost v jednom kanálu na 14,4 kbps. Následným sdružením až 4 timeslotů lze vytvořit kanál s přenosovou rychlostí 14,4 . 4 = 57,6 kbps [10].

EDGE (Enhanced Data Rates for GSM Evolution)

Standard EDGE umožňuje zvýšit přenosovou rychlost systému GSM při alokování všech 8 timeslotů až na hodnotu 384 kbps. Proto byl dříve také označován GSM 384. Standard podporuje paketový přenos dat a přenosová rychlost signálu v jednom timeslotu je 48 kbps. Této vysoké rychlosti je dosaženo vhodnou digitální modulací. Zatímco systémy

GPRS i HSCSD používají modulaci GMSK, systém EDGE používá modulaci 8 PSK (Eight Phase Shift Keying). Využití tohoto standardu proto vyžaduje zásah do hardwarového řešení BTS i MS.

4 ZABEZPEČENÍ PŘENÁŠENÝCH DAT

V dnešní době je velmi důležité chránit přenášená data před neoprávněným přístupem. Z tohoto důvodu je tedy nutné tato data zabezpečit vhodným šifrováním. K tomu se využívají šifrovací (kryptografické) algoritmy. Kryptografické algoritmy rozdělujeme na **systémy symetrické**, které používají k zašifrování a dešifrování stejný klíč a **systémy asymetrické**, které využívají dvou rozdílných klíčů.

4.1 Symetrické kryptosystémy

U symetrických kryptosystémů se používá k šifrování a dešifrování přenášených dat pouze jeden klíč. Komunikující strany musí tudíž tento klíč držet v tajnosti. Velkou výhodou těchto systémů je nízká výpočetní náročnost a tudíž vysoká rychlost šifrování. Jejich velkým problémem je bezpečná distribuce klíčů od zdroje klíčů k odesílateli a příjemci. Symetrické šifry se dělí na **proudové** a **blokové** šifry. V případě proudových šifer hodnota zašifrovaného bitu závisí na hodnotě příslušného bitu zprávy a na hodnotě klíče. V případě blokové šifry hodnota zašifrovaného bitu navíc závisí i na hodnotě dalších bitů dané zprávy. Blokové šifry jsou proto obecně bezpečnější, avšak na druhou stranu proudové šifrátory rychlejší. Mezi nejznámější algoritmy používané v symetrických kryptosystémech patří například algoritmy **DES** (Data Encryption Standard), jeho zesílená varianta **3DES** a z nich vycházející novější algoritmus **AES** (Advanced Encryption Standard) [8].

Algoritmus DES

Algoritmus DES šifruje data v 64-bitových blocích pomocí 56-bitového klíče. Jeho zesílená varianta 3DES pracuje se 168-bitovým klíčem. Nevýhoda tohoto algoritmu je, že může být prolomen hrubou silou (vyzkoušení všech možných klíčů) [8].

Algoritmus AES

Algoritmus AES vychází z principů, které byly použity pro DES. Velký pokrok oproti DES je v délce klíčů. AES podporuje délky klíčů 128, 192 a 256 bitů. Výhoda šifry AES oproti DES je, že jí nehrozí prolomení hrubou silou [8].

4.2 Asymetrické kryptosystémy

U asymetrických systémů se používají dva různé klíče. Jeden z klíčů je tajný a druhý veřejný. Skutečnost, který z klíčů bude tajný, určuje zda kryptografický systém zajišťuje důvěrnost nebo autentičnost. Pokud je veřejným klíčem klíč šifrovací a tajným klíčem klíč dešifrovací, tak kryptogram (zašifrovaný text) může zašifrovat veřejným klíčem kdokoliv, ale dešifrovat jej může pouze majitel tajného klíče. Tím je zajištěna důvěrnost přenesené zprávy. V opačném případě, kdy je veřejným klíčem klíč dešifrovací a tajným klíčem klíč šifrovací, může zprávu zašifrovat pouze majitel tohoto klíče, avšak takovýto kryptogram může veřejným klíčem dešifrovat kdokoliv. Tímto je zaručena autentičnost přenesené zprávy. Mezi výhody systémů s veřejným klíčem patří jednodušší distribuce klíčů, nevýhodou je však značná výpočetní náročnost a tím pádem pomalejší šifrování a dešifrování [8].

4.2.1 RSA

RSA je jedním z nejpoužívanějších asymetrických kryptosystémů. Název RSA je odvozen od jmen tvůrců tohoto kryptosystému (Rivest, Shamir a Adleman). Je založen na problému faktorizace čísla, což je problém rozkladu daného čísla na součin prvočísel [18].

Konstrukce kryptosystému

1. Nalezení dvou velkých prvočísel p a q.
2. Výpočet čísel $n = (p \,.\, q)$, $\varphi = (p-1).(q-1)$.
3. Volba veřejného šifrovacího klíče e. Tento klíč musí být soudělný s číslem r.
4. Výpočet soukromého šifrovacího klíče $d = e^{-1} \bmod \varphi$.
5. Parametry e a n jsou zveřejněny, ostatní parametry nutno uchovat v tajnosti.

Postup šifrování

1. Data jsou rozdělena na bloky o stejné délce. Každý i-tý blok se chápe jako číslo z_i. Musí platit, že $z_i < n$.
2. Jednotlivé bloky z_i jsou poté zašifrovány způsobem: $c_i = z_i^e \bmod n$.
3. Z bloků c_i je následně poskládán kryptogram, který je zaslán adresátovi.

Postup dešifrování

1. Kryptogram je rozdělen na původní bloky c_i.
2. Každý blok c_i je poté dešifrován způsobem: $z_i = c_i^d \bmod n$.
3. Z bloků z_i je následně sestavena původní zpráva.

Při kryptoanalýze RSA má kryptoanalytik k dispozici parametry e a n. K určení soukromého klíče potřebuje znát číslo φ. Prvočísla p a q může získat rozkladem (faktorizací) parametru n. V současné době se používají kryptosystémy, kde n je dlouhé 768, 1024 nebo 2048 bitů. Faktorizace tak velkých čísel je v současné době nereálná. Kryptosystémy RSA umožňují zaručit jak důvěrnost tak i autentičnost. Jejich nevýhodou je však nutnost operací s velkými čísly, což způsobuje značnou pomalost celého kryptosystému [18].

4.2.2 Diffie-Hellman

Oproti kryptosystému RSA nezajišťuje tento protokol vlastní šifrování, ale slouží k bezpečnému vytvoření klíčů pro symetrický kryptosystém prostřednictvím přenosového kanálu. I za podmínky, že útočník odposlechne veškerou komunikaci mezi uživateli, přesto nebude schopen zjistit, jaký klíč byl ustanoven. Je založen na problému nalezení diskrétního logaritmu. Je dána funkce $y = f(x) = g^x \bmod p$, kde prvočíslo p a základ mocniny g jsou známy. Výpočet hodnoty y pro argument x je relativně snadný. Avšak inverzní výpočet, tj. nalezení hodnoty x pro dané y, je výpočetně prakticky nemožný. Právě tento inverzní výpočet se nazývá diskrétní logaritmus [18].

Princip ustanovení klíče

Existuje odesílatel zprávy s označením A a příjemce zprávy s označením B. Dále jsou dány veřejné parametry: velké prvočíslo p a primitivní kořen g.

1. Odesílatel A si zvolí náhodně velké číslo a a příjemce B si zvolí náhodně velké číslo b. Tato čísla musí zůstat v tajnosti.
2. Odesílatel A vypočítá číslo $ALFA = g^a \bmod p$. Obdobně příjemce B vypočítá číslo $BETA = g^a \bmod p$. Vypočtené parametry si přenosovým kanálem mezi sebou předají.
3. Odesílatel A následně vypočítá klíč $K = BETA^a \bmod p$. Příjemce B vypočítá stejnou hodnotu $K = ALFA^b \bmod p$. Klíč K je výsledným klíčem použitelným pro symetrický kryptosystém.

Skutečnost, že oba účastníci vypočítají stejný klíč vyplývá z následující rovnosti:

$$K = BETA^a \bmod p = (g^b)^a \bmod p = (g^a)^b \bmod p = ALFA^b \bmod p$$ [18].

Při kryptoanalýze zná kryptoanalytik veřejné parametry p, g a zná hodnoty $g^a \bmod p$ a $g^b \bmod p$. Ke zjištění klíče ovšem potřebuje zjistit buď tajné číslo a nebo b. K tomu

může využít rovnost $ALFA = g^a \ mod \ p$ nebo $BETA = g^b \ mod \ p$. Tato úloha diskrétního logaritmu však není pro používané hodnoty p o velikosti 768 – 1024 bitů v současné době prakticky řešitelná [18].

4.3 Zabezpečení dat v systémech PLC

Symetrické kryptografické algoritmy mají oproti asymetrickým menší výpočetní náročnost a jsou také jednodušší a levnější. Zároveň je ale u nich obtížné ověřit identitu komunikujícího protějšku a navíc pro komunikaci s n-protějšky je třeba použít n-klíčů. Oproti tomu asymetrické algoritmy sice mají až tisíckrát nižší výpočetní rychlost, ale zároveň u nich lze snadno ověřit identitu protějšku. Navíc díky dvěma klíčům, veřejnému a tajnému, šifrující strana nemusí se stranou dešifrující sdílet žádné tajemství. Tím pádem odpadá nutnost sdílení tajného klíče. Z těchto důvodů se při komunikaci v PLC systémech používají asymetrické algoritmy pro navázání spojení (ustanovení klíčů) a symetrickými algoritmy, které jsou rychlejší, je pak prováděno šifrování přenášených zpráv.

4.4 Zabezpečení dat v systémech GSM/GPRS

Zatímco v pevných sítích se přenáší signály po kabelech, ke kterým je přístup obtížný, u mobilních sítí je signál na cestě k účastníkovi přenášen v rádiovém prostředí, ke kterému má přístup kdokoliv. Proto je třeba přenášené informace zabezpečit proti zneužití nepovolanými osobami. Z důvodu menší výpočetní náročnosti se používají symetrické šifrovací algoritmy. Systém GSM poskytuje čtyři základní způsoby zabezpečení informací:

- použití SIM karty,
- anonymitu, TMSI (Temporary Mobile Subscriber Identity),
- ověření totožnosti,
- ochranu signalizačních a hovorových dat šifrováním.

K tomu se používají následující algoritmy:

- A3 - pro ověření totožnosti účastníka (může být definován operátorem),
- A5 - pro šifrování a dešifrování dat (algoritmus je normalizovaný pro všechny sítě GSM),
- A8 - pro generování šifrovacího klíče (může být definován operátorem) [10].

4.5 Infrastruktura veřejných klíčů

Infrastruktura veřejných klíčů, často označovaná zkratkou PKI, je systém digitálních certifikátů, certifikačních úřadů a dalších registračních úřadů, které slouží k verifikaci a ověření platnosti všech stran zúčastněných v určité elektronické transakci, přičemž je použita kryptografie s veřejným klíčem [19].

4.5.1 Digitální certifikát

Digitální certifikát je datová struktura, která umožňuje zveřejnění údajů o uživateli. Nejdůležitějším údajem zpravidla bývá uživatelův veřejný šifrovací klíč. Uživatel doloží svou identitu certifikační autoritě, která představuje důvěryhodnou třetí stranu. Ta poté certifikát elektronicky podepíše. Certifikát podepsaný certifikační autoritou garantuje, že veřejný klíč v něm obsažen patří určitému uživateli. Všeobecně je užívána struktura certifikátu zavedená doporučením ITU X.509 [20].

4.5.2 Služby PKI

PKI zajišťuje agendu spjatou s fungováním služeb, jako jsou například:

Vytvoření a přidělení nového certifikátu – Zahrnuje především ověření totožnosti žadatele o certifikát. Dále vygenerování páru asymetrických klíčů, vytvoření certifikátů a jejich následné předání žadateli bezpečnou cestou.

Ověřování platnosti certifikátu – Zahrnuje ověření platnosti certifikátu, revokaci (zneplatnění) a zveřejnění seznamu neplatných certifikátů.

Obnovování certifikátu a prodlužování jeho platnosti – U certifikátů, kterým vypršela doba platnosti, zajišťuje prodloužení jejich platnosti [20].

4.5.3 Základní prvky PKI

Certifikační autorita – Představuje důvěryhodnou třetí stranu a předpoklad je, že jí všichni důvěřují. Její hlavní úlohou je především vydávání certifikátů žadatelům.

Registrační autorita – Zajišťuje komunikaci s klienty a ověřuje identitu žadatele o certifikát. Následně provádí registraci žádostí. Registrační autorita může být i součástí certifikační autority, ale většinou to tak není. Registrační a certifikační autorita je základem celé infrastruktury a jejich bezpečnost je klíčová pro bezpečnost celého systému [20].

Repositář - Uchovává a zveřejňuje informace o jednotlivých certifikátech. Vystavuje seznamy revokovaných (zneplatněných) certifikátů.

Držitel certifikátu – Je to subjekt, kterému byl vydán platný certifikát. Tím pádem je s tímto certifikátem jednoznačně spojen a na základě seznamu certifikátů je také jednoznačně identifikovatelný.

Uživatel certifikátu – Je to subjekt, který spoléhá na pravost certifikátu. Na základě ověření pravosti a platnosti certifikátu důvěřuje subjektu, který se identifikuje platným certifikátem [20].

4.6 Distribuce klíčů pomocí PKI

Pro potřeby dálkového měření kvality elektrické energie může být infrastruktura veřejných klíčů využita pro ustanovení a distribuci klíčů do jednotlivých zařízení v síti dálkového měření. Tato zařízení poté mezi sebou mohou díky ustanoveným klíčům komunikovat pomocí symetrické kryptografie.

Ve sběrné síti musí existovat nějaká certifikační autorita. Této autoritě všechna zařízení jako jsou koncentrátory, koncová zařízení i agregační server plně důvěřují a znají její veřejný klíč.

4.6.1 Ustanovení certifikátů

Každému koncovému zařízení, koncentrátoru i agregačnímu serveru jsou před připojením do sítě vystaveny certifikáty, které obsahují jejich jednoznačnou identifikaci a jejich veřejné klíče. Tyto certifikáty jsou poté podepsány certifikační autoritou (zašifrovány jejím soukromým klíčem). Dále je třeba doručit certifikáty jednotlivým zařízením. Doručení by nemělo být prováděno běžnou přenosovou cestou, ale mělo by to být učiněno nějakým důvěryhodným způsobem. Například by jej provedl osobně odpovědný pracovník při instalaci zařízení.

4.6.2 Distribuce klíčů

Distribuce klíčů pro jednotlivá zařízení by s využitím PKI poté mohla probíhat následujícím způsobem:

Ustanovení symetrických klíčů pro komunikaci mezi agregačním serverem a koncentrátory:

Agregační server a jednotlivé koncentrátory si mezi sebou vymění certifikáty. Následně každé ze zúčastněných zařízení ověří platnost certifikátu pomocí veřejného klíče certifikační autority. Agregační server poté vygeneruje *n* různých řetězců dat, kde *n* je počet podřízených koncentrátorů. Tyto řetězce zašifruje veřejnými klíči koncentrátorů, které získal z přijatých certifikátů. Každý ze zašifrovaných řetězců odešle příslušnému

koncentrátoru. Jednotlivé koncentrátory řetězec dešifrují svým soukromým klíčem, následně také vygenerují řetězec dat, zašifrují jej veřejným klíčem agregačního serveru a odešlou mu jej. Agregační server řetězce přijaté z koncentrátorů dešifruje pomocí svého soukromého klíče. Teď má každá ze zúčastněných stran dva řetězce dat, ze kterých pomocí nějakého algoritmu sestaví klíč, který je následně použit pro komunikaci pomocí symetrického šifrování.

Ustanovení symetrických klíčů pro komunikaci mezi koncentrátory a jednotlivými koncovými zařízeními:

Probíhá obdobně, jako v předchozím případě. Každý koncentrátor si se svými podřízenými koncovými zařízeními vymění certifikáty. Následně vygeneruje *n* řetězců dat, kde *n* je počet podřízených koncových zařízení. Tyto řetězce zašifruje veřejnými klíči koncových zařízení. Každý ze zašifrovaných řetězců odešle příslušnému koncovému zařízení. Jednotlivá koncová zařízení řetězec dešifrují svým soukromým klíčem, následně také vygenerují řetězec dat, zašifrují jej veřejným klíčem koncentrátoru a odešlou mu jej. Koncentrátor řetězce, přijaté z koncových zařízení dešifruje pomocí svého soukromého klíče. Teď má opět každá ze zúčastněných stran dva řetězce dat, ze kterých pomocí nějakého algoritmu sestaví klíč, který je následně použit pro komunikaci pomocí symetrického šifrování.

4.7 Zabezpečení sběrných zařízení

Sběrná zařízení, ať už jsou to koncentrátory či agregační servery, obvykle obsahují velké množství citlivých dat, u kterých nechceme, aby byla jakýmkoliv způsobem zneužita. Proto je nutné přístup k těmto datům vhodně zabezpečit. Zabezpečení a autentizace sběrných zařízení se skládá z několika následujících problémů [20].

4.7.1 Autentizace osob při přístupu ke sběrným zařízením

Autentizaci uživatele lze realizovat pomocí různých metod, od přihlašovacích údajů přes nutnost vlastnictví nějakého přístupového hardwaru, jako např. USB token, až po sledování biometrických údajů. Vhodná je také kombinace více těchto metod současně [20].

4.7.2 Autentizace koncových zařízení

Útočník se může vydávat za korektní koncové zařízení, připojit se ke sběrnému zařízení a odesílat falešná data, nebo dokonce využít sestavené spojení k útoku na toto zařízení.

Z těchto důvodů je nutné sběrná zařízení ochránit pomocí autentizace koncového zařízení. Autentizaci lze provést pomocí několika metod. Například na základě přihlašovacích údajů, vlastnictví přístupového hardwaru a nebo na základě certifikátů [20].

4.7.3 Zamezení síťových útoků na sběrná zařízení

Jak ji bylo dříve zmíněno, sběrná zařízení obsahují citlivá data. Proto lze předpokládat, že se útočník bude snažit o provedení nejrůznějších útoků. Snahou útočníka může být odcizení dat, jejich pozměnění, nebo ovlivnění funkčnosti systému. Zabezpečení sběrných zařízení proti těmto útokům může být provedeno například použitím softwarového či hardwarového firewallu [20].

4.8 Zabezpečení koncových zařízení

V dnešní době by se nemělo opomíjet ani zabezpečení koncových zařízení. Koncové zařízení samozřejmě není možno zabezpečit na stejné úrovni jako sběrná zařízení. Ať už z toho důvodu, že jsou koncová zařízení umístěna na mnoha různorodých místech, tak i z toho důvodu, že útočníkem může být v podstatě i uživatel koncového zařízení. Musí se tedy předpokládat, že koncové zařízení je zcela v rukou útočníka. Zabezpečení může být provedeno s využitím několika způsobů [20].

4.8.1 Fyzický přístup do koncového zařízení

Jak již bylo zmíněno, musíme předpokládat, že koncové zařízení je zcela v rukou útočníka. To je velmi obtížně řešitelná situace. V úvahu tedy připadají pouze formy zabezpečení v podobě plomby pro zjištění neoprávněného přístupu nebo manipulace s koncovým zařízením. V krajním případě lze koncové zařízení zkonstruovat tak, aby při pokusu o neoprávněný přístup nebo manipulaci došlo k jeho zničení [20].

4.8.2 Autentizace sběrných zařízení

Koncové zařízení je také nutné ochránit před připojením se k neautorizovanému sběrnému zařízení. Je nutné zajistit, aby koncové zařízení odeslalo data pouze autentizovanému sběrnému zařízení. Autentizaci je možno provést opět na základě přihlašovacích údajů nebo certifikátů [20].

4.8.3 Zamezení síťových útoků na koncové zařízení

Koncové zařízení by dále mělo obsahovat firewall, aby byly eliminovány útoky zahlcením. Při úspěšném útoku by totiž mohlo dojít k blokování komunikace a byl by tak znemožněn odečet dat za příslušné období. Lze také počítat s variantou, kdy bude koncové zařízení součástí firemní sítě. Při této variantě by bylo možné využít firewall,

který je již součástí vybudované sítě. Koncové zařízení by pak obsahovalo pouze jednotku pro šifrovaný přenos dat [20].

4.9 Firemní audity bezpečnosti

Pro kontrolu bezpečnosti sběrné sítě je také možno využít služeb auditorských firem. Pojmem audit bezpečnosti je možné označit prověření něčeho, například sítě a všech jejích prvků z hlediska bezpečnosti, nějakou nezávislou osobou. Výsledky auditu bývají obvykle předávány formou závěrečné zprávy zadavatelům nebo popřípadě zainteresovaným zájemcům [21].

4.9.1 Základní oblasti auditu IT

Audit informačních a komunikačních technologií a informačních systémů můžeme klasifikovat v následujících oblastech:

Bezpečnostní audit (audit IS, penetrační testy) - Cílem bezpečnostního auditu je zmapování aktuálního stavu bezpečnosti, odhalení možných rizik a vytvoření základu pro případné ucelené bezpečnostní řešení [21].

Penetrační testy tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí či zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému. Penetrační testy jsou v podstatě napodobení útoku hackera [22].

Technický audit (audit HW a SW vybavení, audit infrastruktury) - Výstup z této části auditu může obsahovat návrh na rozšíření či úpravu konfigurace systému, případně změnu technologie [21].

Audit informační strategie - Výsledkem je podklad a stanovení kritérií pro správnou strategii v oblasti informačních technologií vzhledem k potřebám a podnikatelským záměrům firmy [21].

Legislativní audit - Sumarizuje základní informace o systému a ověřuje, zda systém je ve shodě s požadavky zákonů, které se týkají bezpečnosti dat a informačních systémů. Mechanismy hodnotící podmínky informačního systému v souladu s požadavky práva [21].

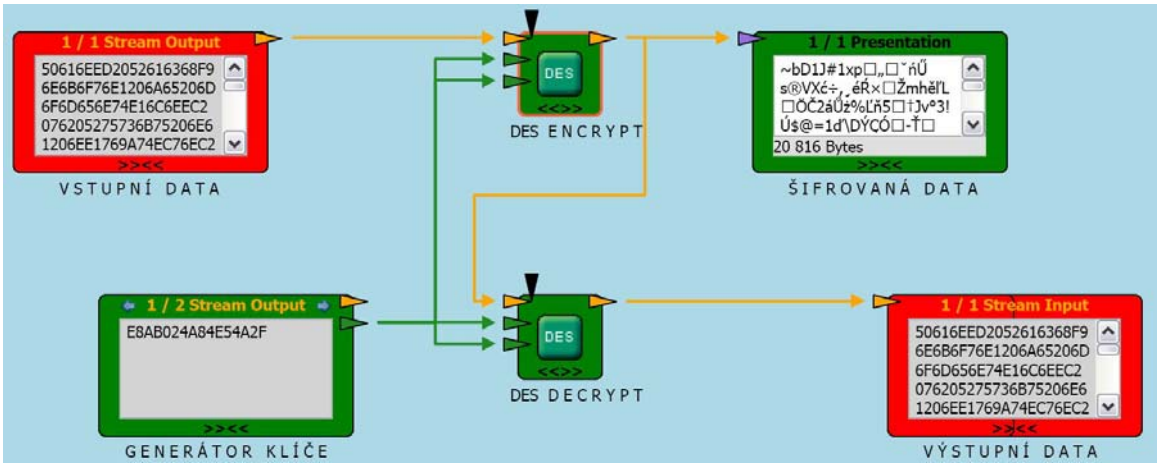
4.9.2 Firmy poskytující auditorské služby

Na českém trhu působí spousta firem, které se zabývají auditem informačních a komunikačních systémů. Jsou to například Risk Analysis Consultants, ESET software spol. s r.o., DCIT, a.s., a další.

5 TESTOVÁNÍ KRYPTOGRAFICKÝCH METOD

Pro zvolení vhodné kryptografické metody určené k přenosu dat z měřičů kvality elektrické energie, bylo nutné učinit srovnání těchto metod. K testování byl použit simulační program Cryptool 2.0, který dokáže analyzovat a simulovat většinu těchto známých kryptografických metod. V této kapitole byla testována časová náročnost šifrování u symetrických kryptografických algoritmů DES, 3DES a AES. Porovnávala se doba zašifrování tří různě velkých textových souborů.

Pro účely testování byly vytvořeny tři textové soubory o velikostech 500 kB, 10 MB a 30 MB. Dále byly v programu Cryptool 2.0 pro každý testovaný algoritmus sestavena bloková schémata. Příklad blokového schéma pro testování algoritmu DES s délkou klíče 64 bitů je znázorněn na obrázku 5.1.

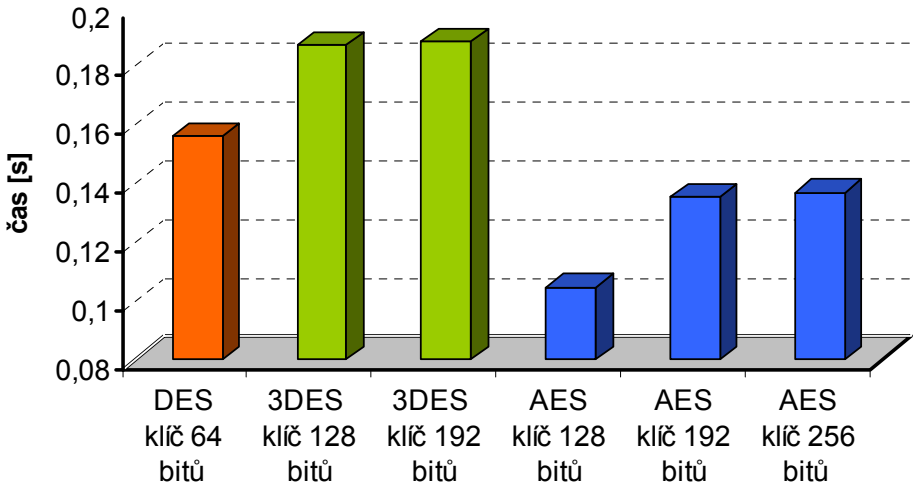


Obrázek 5.1 Schéma pro testování algoritmu DES.

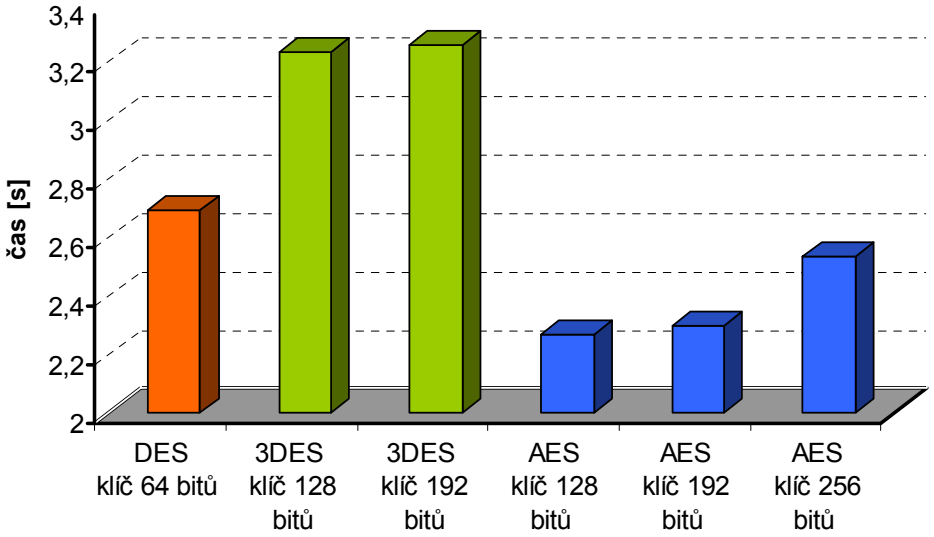
Blok **VSTUPNÍ DATA** sloužil pro načtení testovaného textového souboru. Blok **DES ENCRYPT** provedl zašifrování dat, **DES DECRYPT** poté dešifrování. **GENERÁTOR KLÍČE** dále generoval potřebný 64 bitový klíč. V bloku **ŠIFROVANÁ DATA** jsou pro názornost ještě zobrazeny data z textového souboru v šifrované podobě. Nakonec **VÝSTUPNÍ DATA** ukazují již dešifrované data na výstupu. Pro ostatní testované algoritmy bylo nutné ve schématu změnit šifrovací a dešifrovací bloky a dále pak generátor klíče nastavit na potřebnou hodnotu.

Pro každý z testovaných algoritmů bylo provedeno šifrování a dešifrování všech tří textových souborů, při čemž byla měřena doba, za kterou blok **DES ENCRYPT** zvládne zašifrování. Program CrypTool 2.0 je schopen měřit tuto dobu s přesností na 1 ms. Testování probíhalo na PC s procesorem Intel s frekvencí 1600 MHz a s 1 GB RAM pamětí. Pro přesnější výsledky bylo každé měření provedeno třikrát a následně byla vypočítána průměrná hodnota. Výsledky je možné vidět v grafech 5.2, 5.3, 5.4.

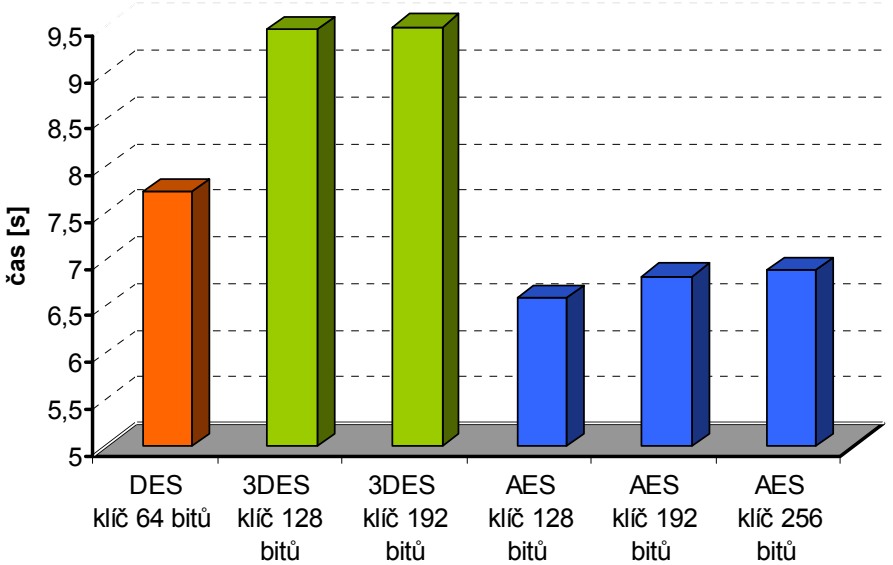
5.1 Grafické zobrazení časové náročnosti kryptografických algoritmů



Obrázek 5.2 Grafické zobrazení časové náročnosti šifrování pro soubor o velikosti 500 kB.



Obrázek 5.3 Grafické zobrazení časové náročnosti šifrování pro soubor o velikosti 10 MB.



Obrázek 5.4 Grafické zobrazení časové náročnosti šifrování pro soubor o velikosti 30 MB.

5.2 Zhodnocení výsledků

Z naměřených hodnot vyplývá, že z hlediska časové náročnosti v testech dopadl nejlépe šifrovací algoritmus AES, větší časová náročnost šifrování byla prokázána u algoritmu DES a nejdelší dobu k zašifrování potřeboval algoritmus 3DES. Stejné pořadí si algoritmy udržely při šifrování testovaných souborů všech tří velikostí. Se zvyšováním délky klíčů se zpoždění doby potřebné k zašifrování projevilo minimálně. Řádově několik jednotek až stovek ms. U algoritmu AES s klíčem délky 128 bitů trvalo zašifrování souboru o velikosti 30 MB v průměru 6,586 sekundy, s klíčem o velikosti 192 bitů pak 6,823 sekundy a při 256-ti bitovém klíči pak 6,888 sekundy. Co se týče bezpečnosti, tak algoritmus AES také splňuje mezinárodní bezpečnostní normy IEC TS 62351-1 [13] a IEC TS 62351-3 [14]. Délka klíče 128 bitů odpovídá mezinárodně uznávanému standardu FIPS 140-2,3 [15] a bude pro naše účely dostačující, protože k prolomení útokem hrubou silou by bylo zapotřebí 2^{128} operací, což za současných podmínek není v reálném čase možné uskutečnit. Když vezmeme v úvahu všechny tyto aspekty, tak algoritmus AES s délkou klíče 128 bitů může být zvolen jako nejvhodnější kryptografický algoritmus pro šifrování přenášených dat z měřičů kvality elektrické energie.

6 GENERÁTOR KRYPTOGRAFICKÝCH KLÍČŮ V PROSTŘEDÍ MATLAB

Pro ustanovení vhodných klíčů pro symetrickou kryptografii, pomocí které jsou šifrováná přenášená data, je dle závěrů z kapitoly 4.3 vhodné použít některou z asymetrických kryptografických metod. Pro praktickou ukázku principů těchto metod byla v rámci této práce vytvořena aplikace pro generování kryptografických klíčů, která umí generovat klíče různých velikostí (64 bitů až 1024 bitů) podle dvou asymetrických kryptografických algoritmů RSA a Diffie-Hellman. Pro realizaci bylo použito prostředí MATLAB, které umožňuje vědeckotechnické výpočty, modelování, návrhy algoritmů, simulace, analýzu a prezentaci dat, paralelní výpočty, měření a zpracování signálů, návrhy řídicích a komunikačních systémů [23].

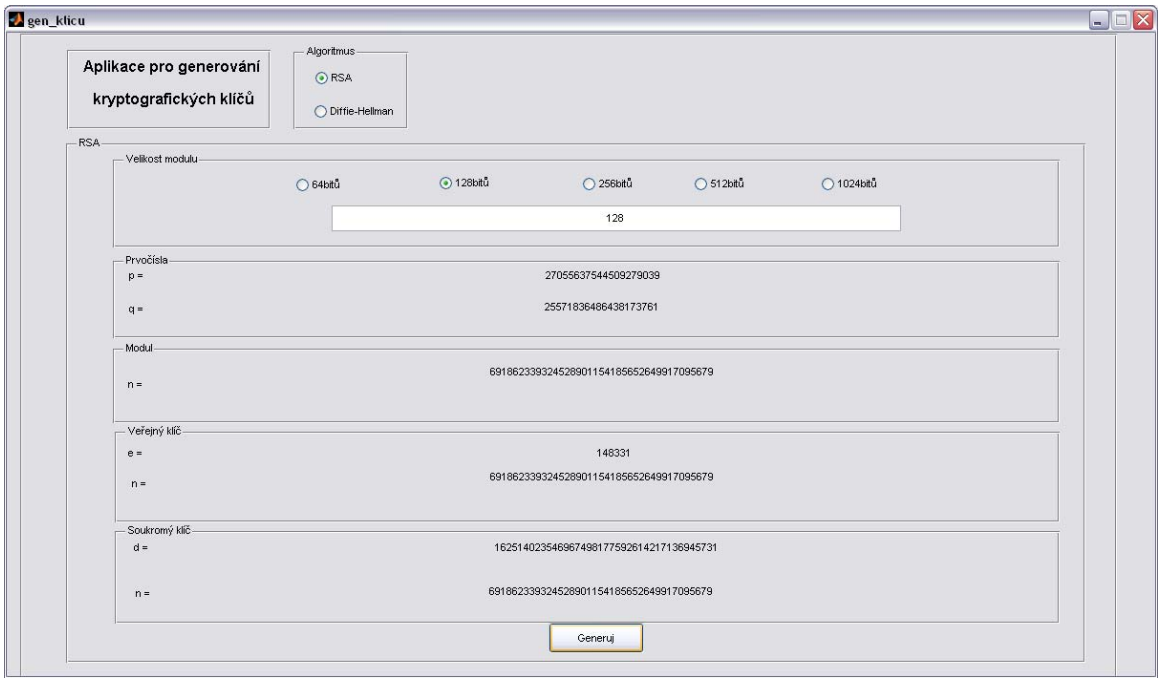
6.1 MAPLE toolbox

Pro bezpečné šifrování dat je nutné používat klíče dostatečné velikosti. U RSA se v dnešní době považují za bezpečné klíče s délkou modulu minimálně 1024 bitů. Zde nastal při realizaci problém, protože prostředí MATLAB ve své základní podobě umí pracovat a matematicky operovat pouze s čísly o maximální velikosti 17 cifer, což je asi 50-ti bitové číslo. To ale nestačí, jelikož k vytvoření 1024 bitového modulu, což je asi 309 cifer, je zapotřebí vynásobit dvě prvočísla o velikosti 512 bitů (asi 155 cifer).

Byly testovány různé metody, jak provádět matematické operace s tak velkými čísly. Z nich se jako nejvhodnější varianta ukázala implementace toolboxu pro matematický software MAPLE. MAPLE je systém počítačové algebry pro využití matematiky v přírodovědných, technických a ekonomických oborech. Umožňuje symbolické a numerické matematické výpočty, jejich počítačovou vizualizaci, dokumentaci a publikaci [24]. Díky MAPLE toolboxu pro MATLAB mohou tato dvě prostředí pracovat dohromady a řešit veškeré problémy. MAPLE toolbox kombinuje symbolické výpočty v MAPLE s numerickými v MATLABu, které se dají společně s výhodou použít pro velmi složité matematické analýzy výsledků. Pomocí toolboxu je k dispozici technické řešení, velmi těsně spjaté s MATLABem, které poskytuje všechny příkazy, vlastnosti a funkce obou programů v jednom fungujícím prostředí [25].

6.2 Popis vytvořené aplikace

Pro spuštění aplikace je nutné mít v prostředí MATLAB implementovaný již výše zmíněný MAPLE toolbox. Bez tohoto toolboxu nebude aplikace fungovat. Aplikace má dva zdrojové soubory *gen_klicu.m* a *gen_klicu.fig*. Pro spuštění aplikace je dále nutné mít oba tyto soubory nahrané v pracovním adresáři MATLABu. Soubor *gen_klicu.m* obsahuje zdrojový kód celé aplikace. V souboru *gen_klicu.fig* je pak uloženo GUI rozhraní, které bylo vytvořeno pro lepší přehlednost a ovladatelnost celé aplikace.



Obrázek 6.1 Aplikace pro generování kryptografických klíčů.

Aplikace se spouští spuštěním souboru *gen_klicu.m*. Otevře se okno vlastní aplikace. V horní části je možno vybrat šifrovací algoritmus, v tomto případě RSA nebo Diffie-Hellman, a velikost modulu. Po stisku tlačítka GENERUJ aplikace vygeneruje klíče dle zvolených parametrů.

7 REALIZACE KRYPTOGRAFICKÝCH ALGORITMŮ V JAZYCE C/C++

Jedním z bodů v zadání této práce bylo vytvořit kryptografické knihovny, pomocí kterých bude možné zabezpečit datovou komunikaci ze sběrných míst dálkového měření. V předchozí kapitole sice byly realizovány kryptografické algoritmy RSA a Diffie-Hellman v prostředí MATLAB, ale pro praktické použití a případnou implementaci do reálných zařízení je vhodné tyto algoritmy realizovat také v jazyce C/C++.

7.1 Knihovna GMP

Při realizaci algoritmů v jazyce C/C++ byl podobně jako v prostředí MATLAB opět řešen problém, jak pracovat a matematicky operovat s velkými čísly. Programovací jazyk C/C++ ve své základní podobě umožňuje pracovat s čísly v rozsahu *-2147483648* až *2147483647* (pro datový typ Int), nebo *0* až *18446744073709551615* (pro datový typ unsigned __int64) [26] . Z důvodů uvedených v kapitole 6.1 toto opět není dostačující. Proto byla použita speciální knihovna GMP, což je speciální knihovna pro práci s libovolně velkými čísly. Neexistuje u ní prakticky žádný limit ve velikosti čísel. Velikost čísel je teoreticky omezena pouze dostupnou pamětí a tak nemusíme mít obavy, že by pro potřeby této práce byly možnosti knihovny nedostačující. GMP knihovna je navržena tak, aby matematické operace prováděla v co nejkratším možném čase a to jak s malými operandy, tak i s velkými. Knihovna je distribuována pod GNU LGPL. Tato licence umožňuje, že knihovnu GMP je možné pro nekomerční účely užívat zdarma [27]. Postup instalace knihovny GMP do programovacího prostředí Code::Blocks je dostupný z [28].

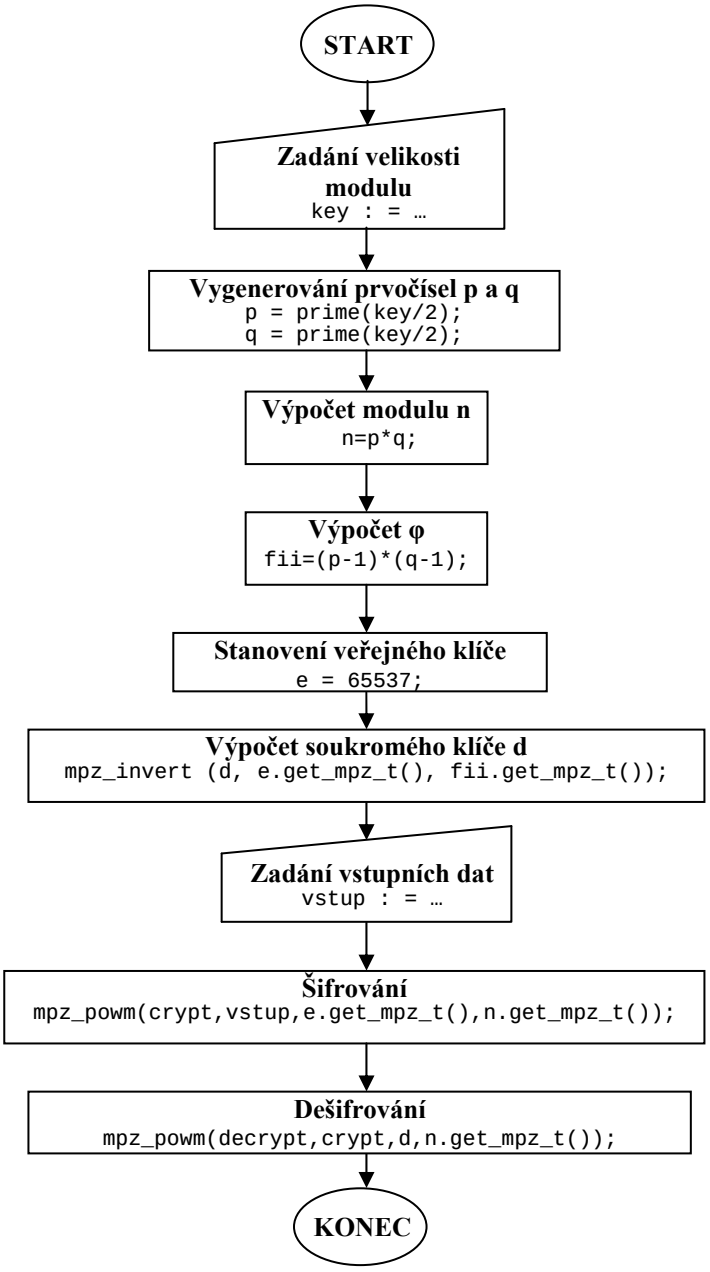
7.2 Realizace algoritmů

Byly realizovány dva asymetrické kryptografické algoritmy RSA a Diffie-Hellman. Realizace probíhala v jazyce C/C++ v prostředí Code::Blocks s využitím již výše zmíněné knihovny GMP. Pro spuštění algoritmů v prostředí Code::Blocks je nutné mít nainstalovanou knihovnu GMP a v parametrech linkeru nastaveno volání knihoven *gmp*, *gmpxx* a *ntl*. Z důvodu větší přehlednosti a možnost odzkoušení funkčnosti algoritmů byly realizovány také konzolové aplikace.

7.3 Realizace algoritmu RSA

Algoritmus RSA byl realizován podle jeho teoretického popisu, který je uveden v kapitole 4.2.1 této práce. Jako veřejný klíč e je nastavena pevná hodnota 65537, která je oblíbenou hodnotou používanou pro veřejné klíče. Je dostatečně velká aby odolávala útokům na malé exponenty a navíc je v binární podobě s výjimkou krajních bitů tvořena samými nulami, což umožňuje efektivní umocňování. Díky využití knihovny GMP je realizovaný algoritmus schopen generovat klíče a šifrovat data prakticky neomezené velikosti. Jednou z podmínek ale je, že délka šifrovaných dat nesmí být větší než délka klíče.

7.3.1 Princip algoritmu



Obrázek 7.1 Zjednodušený diagram algoritmu RSA.

7.3.2 Testování časové náročnosti

Kvůli zjištění časové náročnosti vytvořeného algoritmu byly provedeny testy, při kterých byly měřeny doby trvání jednotlivých funkcí. Testování probíhalo na PC s procesorem Intel s frekvencí 1600 MHz a s 1 GB RAM pamětí. Bylo testováno za jakou dobu je algoritmus schopen vygenerovat klíče o různých velikostech a jakou dobu potřebuje k následnému šifrování a dešifrování bloku dat o velikosti 128 bitů. Výsledky testů ukazuje tabulka 7.1.

Tabulka 7.1 Časová náročnost algoritmu RSA.

Velikost klíče	Doba generování klíče	Doba šifrování a dešifrování
512 *b*	0,094 *s*	0,015 *s*
1024 *b*	0,469 *s*	0,047 *s*
2048 *b*	1,484 *s*	0,250 *s*
4096 *b*	6,750 *s*	1,063 *s*
8192 *b*	12 *min* 44 *s*	5,990 *s*
16384 *b*	1 *hod* 3 *min* 9 *s*	34,672 *s*

7.3.3 Konzolová aplikace

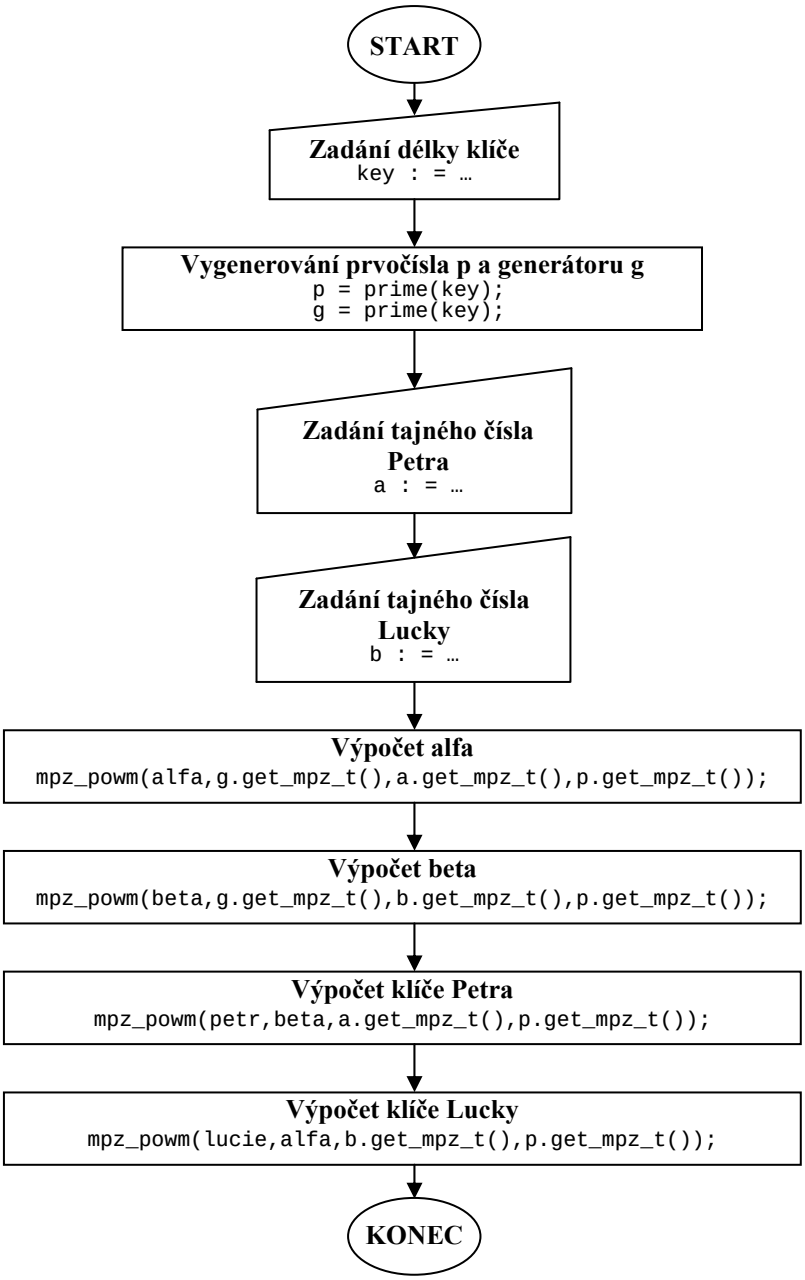
Pro větší přehlednost a možnost odzkoušení funkčnosti algoritmu RSA byla realizována konzolová aplikace. Aplikace se spouští souborem *RSA.exe*. Objeví se vlastní okno aplikace viz obrázek 7.2. Zde se zadá délka modulu v bitech a potvrdí enterem. Aplikace následně vygeneruje klíče dle zvolených parametrů. Poté se zadají vstupní data, které budou šifrovány. Data nesmí být větší, než je velikost vygenerovaného klíče. Po stisku klávesy enter se zobrazí zadaná data, data v šifrované podobě (kryptogram) a dešifrovaná data.

Obrázek 7.2 Okno aplikace RSA.

7.4 Realizace algoritmu Diffie-Hellman

Algoritmus byl realizován podle teoretického popisu, který je uveden v kapitole 4.2.2 této práce. Oproti kryptosystému RSA nezajišťuje tento protokol vlastní šifrování, ale slouží k bezpečnému vytvoření klíčů, které je možné dále použít pro symetrický kryptosystém. Algoritmus je realizován na principu, že dvě komunikující strany, jedna nazvaná jako Petr a druhá jako Lucie, si mezi sebou vyměňují potřebné parametry a následně jsou schopny z těchto parametrů ustanovit jeden stejný klíč. Díky použité knihovně GMP je algoritmus opět schopen generovat klíče prakticky neomezené velikosti.

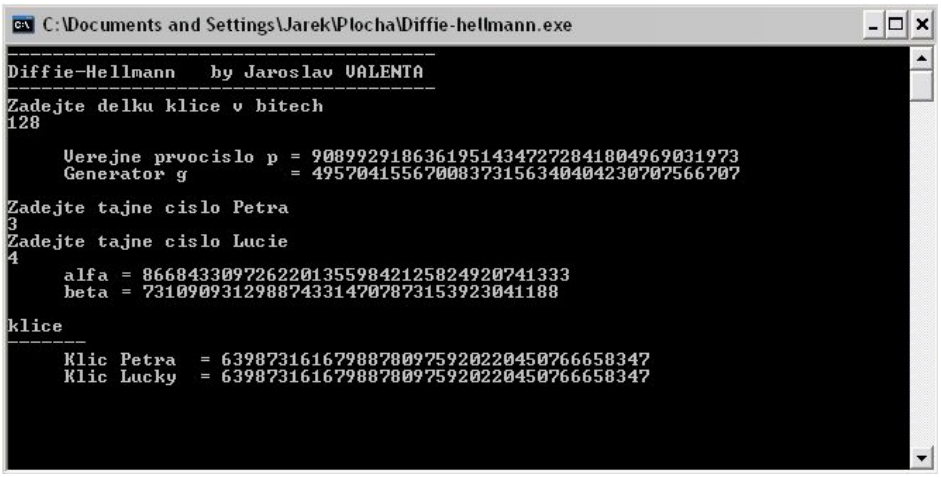
7.4.1 Princip algoritmu



Obrázek 7.3 Zjednodušený diagram algoritmu Diffie-Hellman.

7.4.2 Konzolová aplikace

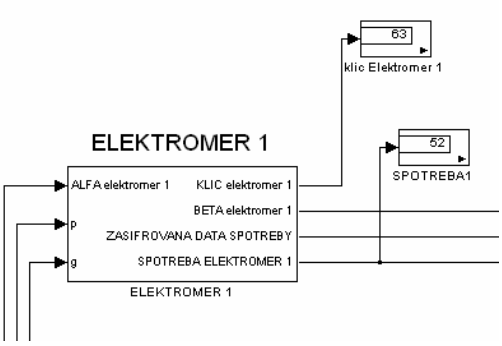
Aplikace se spouští souborem *Diffie-Hellman.exe*. Objeví se vlastní okno aplikace viz obrázek 7.4. Zde se zadá délka modulu v bitech a potvrdí enterem. Následně se zadají veřejná čísla jedné komunikující strany (označena jako Petr) a druhé strany (označena jako Lucie). Aplikace poté vygeneruje identický klíč pro jednu i druhou stranu.



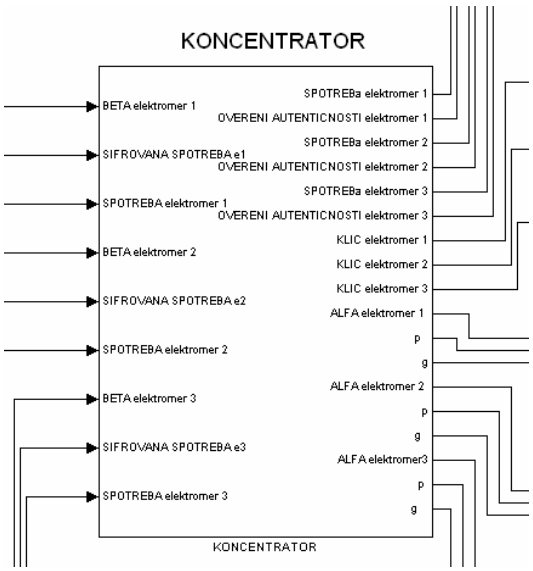
Obrázek 7.4 Okno aplikace Diffie-Hellman.

8 MODEL SBĚRNÉ SÍTĚ V PROSTŘEDÍ MATLAB-SIMULINK

Na základě konceptu systému dálkového měření z kapitoly 2.2, je v rámci této kapitoly v prostředí MATLAB-SIMULINK realizován simulační model sběrné sítě dálkového měření kvality elektrické energie. Model řeší datovou komunikaci mezi koncovými zařízeními (elektroměry) a sběrným zařízením (koncentrátorem). Tato komunikace by v reálném prostředí probíhala pomocí technologie PLC. Jedním z velkých problémů, se kterými je při přenosu naměřených dat nutno počítat, je zabezpečení těchto dat proti jejich pozměnění. Proto byl v rámci modelu řešen především problém, jakým způsobem zabezpečit autentičnost dat. Jinými slovy jak zabezpečit to, že data, která přišla z koncového zařízení do sběrného zařízení, opravdu pochází z příslušného koncového zařízení a nebyla při vlastním přenosu nějakým způsobem pozměněna.



Obrázek 8.1 Koncové zařízení.



Obrázek 8.2 Sběrné zařízení.

8.1 Popis modelu

Nejprve se bylo nutno vypořádat se zabezpečením autentičnosti přenášených dat. To je možno zabezpečit pomocí různých typů šifrování. V kapitole 4.3 této práce již bylo řečeno, že jako nejvhodnější způsob pro šifrování přenášených dat po PLC je vhodné použít asymetrické kryptografické metody pro ustanovení klíčů a dále pak některou se symetrických kryptografických metod pro vlastní přenos dat. Z této skutečnosti bylo také vycházeno i při tvorbě tohoto simulačního modelu. Pro ustanovení klíčů byl zvolen Diffie-Hellmanův kryptografický protokol. Pro vlastní šifrování pak z důvodu jednoduchosti a názornosti jednoduchá proudová šifra.

8.1.1 Ustanovení klíčů

K ustanovení klíčů je využit Diffie-Hellmanův kryptografický protokol. Dle tohoto protokolu si sběrná zařízení a koncová zařízení vymění potřebné parametry a následně ustanoví kryptografické klíče. V rámci modelu jsou pro názornost a výpočetní jednoduchost volena malá čísla. V reálných podmínkách by tato čísla samozřejmě dostatečná nebyla. Proto by se do koncových zařízení i sběrného zařízení implementoval algoritmus pro Diffie-Hellmanův protokol v jazyce C/C++, který byl vytvořen v rámci této práce a v kapitole 7.4.

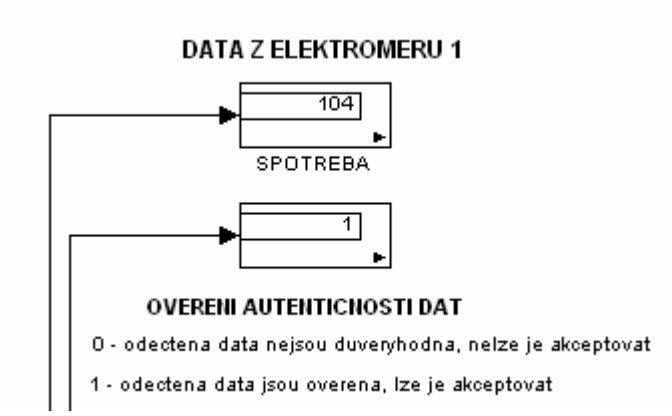
8.1.2 Přenos dat

Z koncových zařízení jsou naměřené údaje přenášeny do sběrného zařízení. Data jsou přenášena jak v normální, tak v zašifrované podobě a to z důvodu ověření jejich autentičnosti. Každé koncové zařízení obsahuje jednoduchý šifrátor, který provádí šifrování tak, že vezme naměřená data a ustanovený klíč a provede s nimi operaci XOR. Následně pak odešle data v normální i zašifrované podobě do sběrného zařízení. Sběrné zařízení obsahuje blok ověření autentičnosti, který pomocí funkce XOR a ustanoveného klíče zašifrovaná data opět dešifruje a následně porovná s přijatými daty v normální podobě. Pokud jsou data stejná, jsou akceptována a je záruka, že během přenosu nebyly pozměněny. Jednoduchá proudová šifra je opět volena jen z důvodu názornosti a výpočetní nenáročnosti. V reálných podmínkách by byl na základě skutečností zjištěných v kapitole 5 použit symetrický kryptografický algoritmus AES, který sice nebyl v rámci této práce realizován, ale je volně dostupný z [29].

8.2 Spuštění modelu

K úspěšnému spuštění je nutné mít nainstalováno prostředí MATLAB. Model se skládá ze dvou souborů. M-file *generovani_dat.m* a vlastní soubor modelu *model_sberne_site.mdl*. Nejprve je nutné spustit m-file *generovani_dat.m*.Ten vygeneruje potřebná prvočísla a konstanty nutné ke stanovení kryptografických klíčů. Dále se stará o generování naměřených dat jednotlivých měřicích míst. Následně je možné spustit vlastní model. Po stisknutí tlačítka PLAY se pomocí bloků from_workspace nahrají vygenerované konstanty z pracovního prostoru MATLABU do modelu. Poté se na jednotlivých displejích zobrazí patřičné hodnoty. Klíče vygenerované v jednotlivých koncových zařízeních by měly odpovídat příslušným klíčům vygenerovaným ve sběrném zařízení. Dále hodnoty spotřeby u jednotlivých elektroměrů by měly odpovídat hodnotám odečteným ve sběrném zařízení.

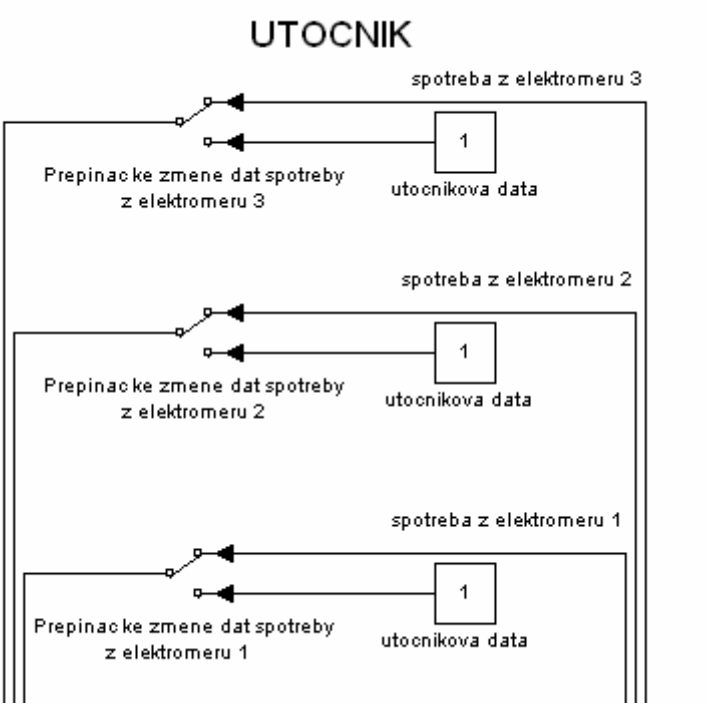
Displej ověření autentičnosti signalizuje, zda-li je u odečtených dat ověřena autentičnost. Autentičnost se ověřuje podle způsobu popsaném v předchozí podkapitole 8.1.2. Pokud displej zobrazuje stav "1", pak je u odečtených dat ověřena autentičnost a lze je akceptovat, pokud je zobrazen stav "0", pak byla odečtená data během přenosu pozměněna a nelze je brát v potaz.



Obrázek 8.3 Displej ověření autentičnosti.

8.2.1 Simulace útoku

Pro simulaci útoku, spočívajícím ve změně dat během přenosu, je v modelu určena část, která simuluje práci útočníka.



Obrázek 8.4 Simulace útočníka.

Útok spočívá v nahrazení přenášených dat vlastními daty útočníka. Tato část se skládá ze 3 přepínačů a dat útočníka. Přepnutím přepínače jsou nahrazena data z elektroměru

vlastními daty útočníka. Po stisknutí tlačítka PLAY tato falešná data doputují do sběrné centrály. Centrála však díky bloku ověření autentičnosti zjistí, že data nepochází z příslušného elektroměru, tudíž na displeji autentičnosti se zobrazí stav “0“ a přijatá data tak nejsou akceptována.

Obrázek 8.5 Ověření autentičnosti.

ZÁVĚR

V této práci byly rozebrány parametry kvality elektrické energie. Byly popsány systémy dálkového měření AMR, AMM a AMI. Dále byly testovány a rozebrány různé druhy kryptografických algoritmů. Z testování vyplynulo, že z hlediska časové náročnosti v testech dopadl nejlépe šifrovací algoritmus AES, větší časová náročnost šifrování byla prokázána u algoritmu DES a nejdelší dobu k zašifrování potřeboval algoritmus 3DES. Stejné pořadí si algoritmy udržely při šifrování testovaných souborů všech tří velikostí. Co se týče bezpečnosti, tak algoritmus AES také splňuje mezinárodní bezpečnostní normy IEC TS 62351-1 [13] a IEC TS 62351-3 [14]. Délka klíče 128 bitů také odpovídá mezinárodně uznávanému standardu FIPS 140-2,3 [15] a bude pro naše účely dostačující, protože k prolomení útokem hrubou silou by bylo zapotřebí 2^{128} operací, což za současných podmínek není v reálném čase možné uskutečnit. S přihlédnutím ke všem těmto aspektům byl algoritmus AES s délkou klíče 128 bitů zvolen jako nejvhodnější kryptografický algoritmus pro šifrování přenášených dat z měřičů kvality elektrické energie. V prostředí MATLAB byla pro ukázku principů asymetrických kryptografických algoritmů RSA a Diffie-Hellman vytvořena aplikace generátoru klíčů. Pro praktické použití a případnou implementaci do reálných zařízení byly tyto dva kryptografické algoritmy realizovány také v jazyce C/C++. V obou vývojových prostředí se podařilo vypořádat se s problémy matematických operací s velkými čísly, tudíž algoritmy generují bezpečné klíče dostatečných délek. U generátoru v prostředí MATLAB byla testována maximální délka klíče 2048 bitů, algoritmy realizované v C/C++ umožňují díky použité knihovně GMP generovat klíče libovolných velikostí. Velikost je teoreticky omezena pouze výpočetní kapacitou použitého hardwaru. Dále byl navržen koncept systému dálkového měření kvality elektrické energie. Navržený systém využívá prvky systému ISAR od firmy *ModemTec* v kombinaci s měřiči kvality elektrické energie PQmetr od firmy *MEgA*. V navrženém systému jsou využity technologie PLC a GPRS, které byly v této práci rovněž popsány. Na základě tohoto konceptu byl v poslední části práce realizován simulační model sběrné sítě dálkového měření kvality elektrické energie. Model simuluje datovou komunikaci mezi sběrným zařízením a koncovými zařízeními. Obsahuje ustanovení kryptografických klíčů, šifrování i samotný přenos dat. Je přidán i model útočníka, který simuluje pozměnění přenášených dat během přenosu.

SEZNAM POUŽITÉ LITERATURY

[1] Kvalita napětí v energetických soustavách průmyslových podniků. *Elektrotechnický magazín*. 2006, 1.

[2] Elektrika.cz [online]. [cit. 2010-10-11]. *Parametry kvality napětí.* Dostupné z WWW: <http://elektrika.cz/terminolog/eterminologitem.2005-05-27.1663394665/view?searchterm=Kvalita%20nap%C4%9Bt%C3%AD>.

[3] E.ON [online]. 2010 [cit. 2010-10-18]. www.eon.cz. Dostupné z WWW: <http://www.eon.cz/cs/info/parameters.shtml#4>.

[4] ČSN EN 50160 : *Charakteristiky napětí elektrické energie dodávané z veřejné distribuční sítě.*

[5] MAREŠ, Pavel. *Systémové řešení v oblasti měření kvality elektrické energie.* Elektro [online]. 2010, 5, [cit. 2010-10-20]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=41162>.

[6] *Smart metering systems.* In Smart metering systems [online], [cit. 2010-10-19]. Dostupné z WWW: <http://m-c-energy.eu/Smart_Metering_Systems.pdf>.

[7] *AMM-automatický systém pro řízení dodávek energií.* In www.zpa.cz [online], [cit. 2010-10-21]. Dostupné z WWW: <http://www.zpa.cz/index.php/cz/content/download/392/2603/file/Článek-AMM.pdf >.

[8] VALENTA, J. *Úzkopásmový přenos dat po energetických sítích*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 50 s. Vedoucí bakalářské práce Ing. Petr Mlýnek.

[9] PETERKA, Jiří. *Data v mobilních sítích : Celulární princip*. Softwarové noviny [online]. 2000, 8, [cit. 2010-10-27]. Dostupný z WWW: <http://www.earchiv.cz/a008s200/a008s201.php3>.

[10] HANUS, Stanislav. *Rádiové a mobilní komunikace*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií.

[11] www.modemtec.cz [online]. [cit. 2010-11-12]. *ISAR.* Dostupné z WWW: <http://www.modemtec.cz/isar.php>.

[12] http://e-mega.cz/ [online]. [cit. 2010-11-12]. *PQmonitor.* Dostupné z WWW: <http://e-mega.cz/doc/pqmonitor_mail.pdf>.

[13] IEC 62351-1*, Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

[14] IEC 62351-3*, Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

[15] FIPS PUB 140-2 - "*Security Requirements for Cryptographic Modules*" National Institute of Standards and Technology, May 25, 2001.

[16] Landis+Gyr [online]. [cit. 2010-11-11]. Dostupné z WWW: <http://www.landisgyr.com/>.

[17] Actaris s.r.o. [online]. 2010 [cit. 2010-11-11]. Dostupné z WWW: <http://www.actaris.cz/>.

[18] BURDA, Karel.: *Bezpečnost informačních systémů*. Skripta FEKT VUT v Brně, 2005.

[19] Microsoft TechNet [online]. 2011 [cit. 2011-05-09]. *Infrastruktura veřejných klíčů*. Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc757327(WS.10).aspx>.

[20] POPELKA, Antonín. *Metody autentizace sběrové centrály* [online]. Brno, 2006. Projekt MPO ČR evid. č. FT-TA2/073. AIS spol. s r. o. Dostupné z WWW: <http://www.ais-brno.cz/vyvoj/zprava_09.pdf>.

[21] NĚMEC, Petr. *Audit informačních systémů nebo penetrační testy?*. Konference Systémová integrace 2011 [online]. 2008, [cit. 2011-05-10]. Dostupný z WWW: <http://si.vse.cz/archive/proceedings/2008/audit-informacnich-systemu-nebo-penetracni-testy.pdf>.

[22] Svět sítí [online]. 2007-10-28 [cit. 2011-05-10]. *Penetrační testy v bezpečnostní analýze informačního systému.* Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=309>.

[23] Humusoft.cz [online]. 2011 [cit. 2011-04-20]. *MATLAB, Simulink.* Dostupné z WWW: <http://www.humusoft.cz/produkty/matlab/>.

[24] Maplesoft.cz [online]. 2011 [cit. 2011-04-20]. *Maple.* Dostupné z WWW: <http://www.maplesoft.cz/maple>.

[25] Maplesoft.cz [online]. 2011 [cit. 2011-04-20]. *Maple Toolbox for Matlab.* Dostupné z WWW: <http://www.maplesoft.cz/toolbox-for-matlab>.

[26] Msdn.microsoft.com [online]. 2011 [cit. 2011-05-01]. *Data Type Ranges.* Dostupné z WWW: <http://msdn.microsoft.com/en-us/library/s3f49ktz(v=vs.80).aspx>.

[27] *The GNU MP Bignum Library* [online]. 2011 [cit. 2011-05-01]. Dostupné z WWW: <http://gmplib.org/>.

[28] Karlin.mff.cuni.cz/~stanovsk [online]. 2011 [cit. 2011-05-01]. *Postup instalace Code::Blocks a knihoven GMP & NTL ve windows 7.* Dostupné z WWW: <http://www.karlin.mff.cuni.cz/~stanovsk/vyuka/instalace.htm>.

[29] Hoozi.com [online]. 2011 [cit. 2011-05-05]. *Advanced Encryption Standard (AES) Implementation in C/C++ with comments.* Dostupné z WWW: <http://www.hoozi.com/post/829n1/advanced-encryption-standard-aes-implementation-in-c-c-with-comments-part-1-encryption>.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH ZKRATEK

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMM	Automated Meter Management
AMR	Automated Meter Reading
BTS	Base Transceiver Station
CENELEC	European Committee for Electrotechnical Standardization
DES	Data Encryption Standard
EDGE	Enhanced Data Rates for GSM Evolution
EN	Evropská Norma
ETSI	European Telecommunications Standards Institute
F	Full Rate
FFT	Fast Fourier Transform
FIPS	Federal Information Processing Standards
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
H	Half Rate
HDO	Hromadné Dálkové Ovládání
HSCSD	High Speed Circuit Switched Data
HW	Hardware
IEC TS	International Electrotechnical Commission Technical Specification
IS	Informační Systém
IT	Information Technology
ITU	International Telecommunication Union
MS	Mobile Station
NN	Nízké Napětí
PKI	Public Key Infrastructure
PLC	Power Line Communication
PSK	Phase Shift Keying
RAM	Random Access Memory
SW	Software
TCP	Transmission Control Protocol
THD	Total Harmonic Distortion

TCH	Traffic Channel
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
VN	Vysoké Napětí
VPN	Virtual Private Network
VVN	Velmi Vysoké Napětí
XML	Extensible Markup Language

OBSAH PŘILOŽENÉHO CD

Přiložené CD obsahuje vlastní text diplomové práce, dále pak simulační model sběrné sítě a všechny aplikace i algoritmy, které byly v rámci diplomové práce vytvořeny.

Adresářová struktura

Přiložené CD obsahuje následující adresáře:

Diplomová práce

V tomto adresáři je uložena diplomová práce ve formátu pdf.

Kryptografické algoritmy C

Adresář obsahuje zdrojové soubory realizovaných kryptografických algoritmů RSA a Diffie-Hellman. Algoritmy byly realizovány v jazyce C++ v prostředí Code::Blocks v8.02. Pro úspěšnou kompilaci je mít třeba nainstalovánu knihovnu GMP a v parametrech linkeru nastaveno volání knihoven *gmp*, *gmpxx* a *ntl*. Z důvodu odzkoušení funkčnosti algoritmů i na PC, na kterých nejsou prostředí Code::Blocks a knihovna GMP nainstalovány, byly vytvořeny spustitelné aplikace *RSA.exe* a *Diffie-Hellman.exe*, které rovněž adresář obsahuje.

Generátor klíčů MATLAB

Adresář obsahuje zdrojové soubory aplikace pro generování kryptografických klíčů. Aplikace byla vytvořena v prostředí MATLAB verze 7.1.0.246 (R14) Service Pack 3. Pro spuštění aplikace je nutné mít v prostředí MATLAB implementovaný MAPLE toolbox. Bez tohoto toolboxu nebude aplikace fungovat. Aplikace se skládá ze dvou zdrojových souborů *gen_klicu.m* a *gen_klicu.fig*. Pro spuštění aplikace je dále nutné mít oba tyto soubory nahrané v pracovním adresáři MATLABu. Aplikace se spouští spuštěním m-filu *gen_klicu.m.*

Model sběrné sítě

Adresář obsahuje soubory modelu sběrné sítě. K úspěšnému spuštění je nutné mít nainstalováno prostředí MATLAB. Model se skládá ze dvou souborů. M-file *generovani_dat.m* a vlastní soubor modelu *model_sberne_site.mdl*. Nejprve je nutné spustit m-file *generovani_dat.m*. Ten vygeneruje potřebné hodnoty. Následně je možné spuštěním souboru *model_sberne_site.mdl* spustit vlastní model.